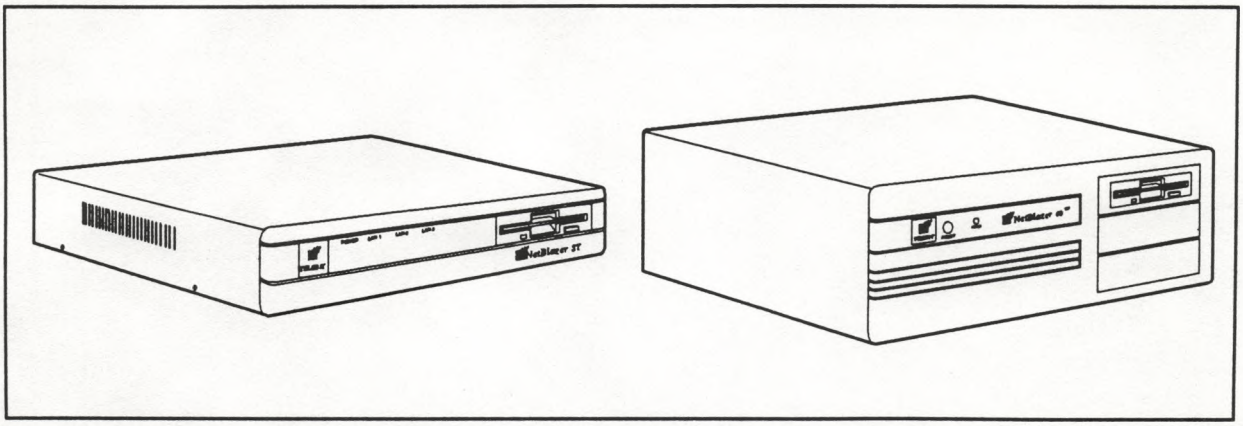
NetBlazer®

Installation and Configuration Guide

TELEBIT®
First In Dial-Up Networking

Installation Guide



NetBlazer

Installation Guide

90270-01

Trademarks

Telebit, NetBlazer, and TrailBlazer are trademarks of Telebit Corporation.

Telebit gratefully acknowledges the following additional copyrights:

- Apple and AppleTalk are registered trademarks of Apple Computer, Inc.
- Novell and NetWare are registered trademarks of Novell, Inc.
- UNIX is a registered trademark of AT&T Bell Laboratories.
- TCL is copyrighted by the University of California, Berkeley (unrestricted redistribution).

Other brands or product names are trademarks or registered trademarks of their respective holders.

Software Copyright Notice

This product contains software which has been copyrighted by Telebit Corporation, Sunnyvale, CA. All rights are reserved.

YOUR RIGHTS OF OWNERSHIP ARE SUBJECT TO THE LIMITATIONS AND RESTRICTIONS IMPOSED BY THE COPYRIGHT LAWS (TITLE 17, UNITED STATES CODE).

IT IS AGAINST THE LAW TO COPY, REPRODUCE, OR TRANSMIT (INCLUDING, WITHOUT LIMITATION, ELECTRONIC TRANSMISSION OVER ANY NETWORK) ANY PART OF THE SOFTWARE.

THIS IS NOT A FULL STATEMENT OF THE COPYRIGHT LAWS. FOR A COMPLETE STATEMENT OF THE RESTRICTIONS IMPOSED ON YOU UNDER THE COPYRIGHT LAWS OF THE UNITED STATES, SEE TITLE 17, UNITED STATES CODE.

Limitation of Warranty and Liability

Telebit Corporation has prepared this document for use by Seller's personnel, customers, and licensees. The information contained in it is the property of Telebit Corporation and shall not be copied, photocopied, translated or reproduced in any electronic or machine readable form, either in whole or in part, without the written approval of Telebit Corporation.

Telebit Corporation or Seller shall not be responsible for any loss, cost, or damage caused by reliance on these materials. Telebit Corporation reserves the right to, without notice, modify or revise all or part of this document and/or change product features or specifications.

Telebit, Seller, or any dealer distributing this product, makes NO WARRANTY, EXPRESSED or IMPLIED, with respect to this manual, and any related items, its quality, performance, merchantability, or fitness for any particular use. It is solely the purchaser's responsibility to determine its suitability for any particular purpose.

Telebit Corporation and Seller will in no event be held liable for direct, indirect, or incidental damages resulting from any defect or omission in this manual, or any other related items and processes, including, but not limited to, any interruption of services, loss of business or anticipatory profits, or other consequential damages.

Copyright © 1993 Telebit Corporation.

Printed in U.S.A.

How to Use This Manual

This manual is a guide to installing the NetBlazer hardware. It is intended to be used by the network administrator or technican/engineer responsible for hardware installation.

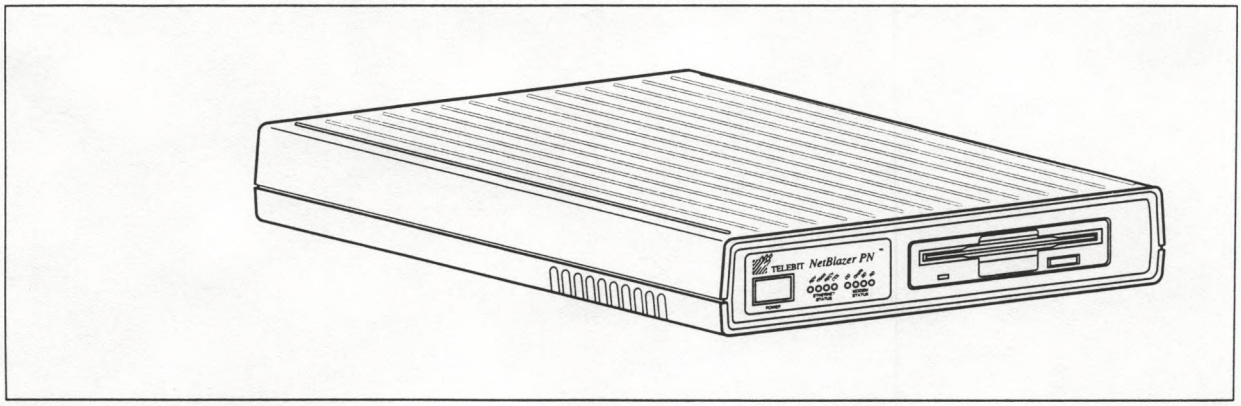
This manual covers three NetBlazer models: the NetBlazer PN, the NetBlazer ST, and the NetBlazer 40. It also covers the Telebit family of NetBlazer Option boards. This manual is structured to directly reflect the NetBlazer products and options as four separate Installation Guides:

- *1, NetBlazer PN Installation Guide*
- *2, NetBlazer ST Installation Guide*
- *3, NetBlazer 40 Installation Guide*
- *4, NetBlazer Option Boards Installation Guide*

Related Documentation

Once the installation of the NetBlazer hardware has been completed, you are ready to perform the software configuration. This procedure involves establishing the IP, IPX, or AppleTalk addresses, routes, and users for the NetBlazer and is covered in the *NetBlazer Configuration Guide*.

A complete listing of the NetBlazer's commands, along with comprehensive descriptions and examples of usage, is contained in the *NetBlazer Command Reference* manual.



NetBlazer PN

Installation Guide

90271-01

March, 1993

Trademarks

Telebit, NetBlazer, and TrailBlazer are trademarks of Telebit Corporation.

Other brands or product names are trademarks or registered trademarks of their respective holders.

Software Copyright Notice

This product contains software which has been copyrighted by Telebit Corporation, Sunnyvale, CA. All rights are reserved.

YOUR RIGHTS OF OWNERSHIP ARE SUBJECT TO THE LIMITATIONS AND RESTRICTIONS IMPOSED BY THE COPYRIGHT LAWS (TITLE 17, UNITED STATES CODE).

IT IS AGAINST THE LAW TO COPY, REPRODUCE, OR TRANSMIT (INCLUDING, WITHOUT LIMITATION, ELECTRONIC TRANSMISSION OVER ANY NETWORK) ANY PART OF THE SOFTWARE.

THIS IS NOT A FULL STATEMENT OF THE COPYRIGHT LAWS. FOR A COMPLETE STATEMENT OF THE RESTRICTIONS IMPOSED ON YOU UNDER THE COPYRIGHT LAWS OF THE UNITED STATES, SEE TITLE 17, UNITED STATES CODE.

Limitations

The information contained in this document was accurate at the time of printing; however, Telebit Corporation assumes no liability for errors or omissions.

In keeping with a philosophy of continual product improvement, Telebit also reserves the right to make changes at any time without notice.

Copyright © 1993 Telebit Corporation.

Printed in U.S.A.

FCC Warning

This equipment generates and uses radio frequency energy, and if not installed and used in strict accordance with the instructions in this manual, may cause interference to radio and television reception. It has been tested and found to comply with the limits for a Class A computing device under Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference in a commercial installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the system on and off, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna
- Relocate the system with respect to the receiver
- Move the system away from the receiver
- Plug the system into a different outlet so that the system and receiver are on different branch circuits

If necessary, consult your dealer or any experienced radio/television technician for additional suggestions. You may find a booklet prepared by the FCC entitled *How to Identify and Resolve Radio-TV Interference Problems* helpful in resolving any problems. This booklet is available from the U.S. Government Printing Office, Washington DC 20402, Stock Number 004-000-00345-4.

How to Use This Manual

This manual is a guide to installing the NetBlazer PN hardware. It is intended for use by the network administrator, technician, or engineer responsible for hardware installation.

Two models of the NetBlazer PN are available. One model contains an internal modem and one serial port, the other two serial ports and no internal modem. You must specify which model you want when you make the initial order. This manual covers both models.

This manual consists of three chapters:

- Chapter 1, Introduction, provides an overview of the NetBlazer PN product, its features, and its applications. It also provides some basic product specifications.
- Chapter 2, Preinstallation Planning, reviews the cable configurations and related information about the environment in which the NetBlazer PN will be operating that you will need to know before beginning the actual installation.
- Chapter 3, NetBlazer PN Installation, details the procedures required to perform the physical and electrical connection of the NetBlazer PN to its respective peripheral devices and "the outside world."

Related Documentation

Once the installation of the NetBlazer PN has been completed, you are ready to perform the software configuration. This procedure involves establishing the IP, IPX or AppleTalk addresses, routes, and users for the NetBlazer PN and is covered in the *NetBlazer Configuration Guide*.

If you are putting the NetBlazer PN on an IPX network, Telebit recommends that you use the NetBlazer Configuration Utility to configure the NetBlazer PN. However, a command line interface may also be used in all other cases. The Getting Started step-by-step configuration procedure described in the *NetBlazer Configuration Guide* is generally adequate for the majority of users. However, extensive customization of a broad range of operational parameters is available to system administrators who wish to take advantage of the NetBlazer's rich capabilities. These facilities are also described in the *NetBlazer Configuration Guide*.

A complete listing of the NetBlazer's commands, along with comprehensive descriptions and examples of usage, is contained in the *NetBlazer Command Reference* manual.

Descriptions of the modem "AT" commands for the PN1 are available on the Telebit FTP Server. Refer to the appendix in the *NetBlazer Command Reference* manual that covers update procedures for information on obtaining a list of the PN1 modem "AT" commands.

Table of Contents

Introduction

Product Profile 1-1
Description 1-2
Model PN1 1-3
Model PN2 1-3
Specifications–NetBlazer PN 1-4
Models 1-4
Electrical 1-4
Physical 1-4
Weight 1-4
Environmental 1-4
Internal Modem (PN1 only) 1-4
Serial Port(s) 1-4
Ethernet Port 1-5
Accessories Furnished 1-5

Preinstallation Planning

General Planning 2-1
Ethernet Requirements 2-1
Synchronous Interface Requirements 2-1
External Modem Requirements 2-2
Configuration Methods and Considerations 2-4
Using the NetBlazer Configuration Utility 2-4
Using the NetBlazer's AppleTalk Interface 2-4
Using the NetBlazer's Command Line Interface 2-4
Using DOS to Preconfigure the NetBlazer 2-5
Administrator's Workstation Requirements 2-5

NetBlazer PN Installation

Connecting the Ethernet Port 3-1
Connecting the NetBlazer PN to a Thin Ethernet (10Base2) Network 3-2
Connecting the NetBlazer PN to a Thick Ethernet (10Base5) Drop 3-2
Connecting the NetBlazer PN to an RJ-45 Twisted Pair (10BaseT) 3-3
Connecting the Synchronous Port 3-4
Connecting the Asynchronous Ports (External Modems) 3-4
Connecting the Internal Modem 3-5
Administrator's Workstation 3-5
Connecting a Dial-in Administrator's Workstation 3-6
Connecting a Local Administrator's Workstation 3-6
Connecting the AC Power Supply 3-6

Appendix A, NetBlazer PN POST Codes

Appendix B, Interface Port Pinout Data

Introduction 1

This manual provides instructions and related information required to install the NetBlazer PN. It is intended to be used by service personnel and qualified network administrators.

The Product Profile section of this chapter describes the applications for which the NetBlazer PN is best suited. The Specifications–NetBlazer PN section of this chapter provides basic electrical, physical, and environmental specifications. It also provides a list of available options and defines the elements on the NetBlazer PN's front and rear panels.

Product Profile

The NetBlazer PN is the most compact member of the NetBlazer family (see Figure 1-1). Featuring lowest cost and smallest footprint of the NetBlazer products, the NetBlazer PN supports standard NetBlazer software.

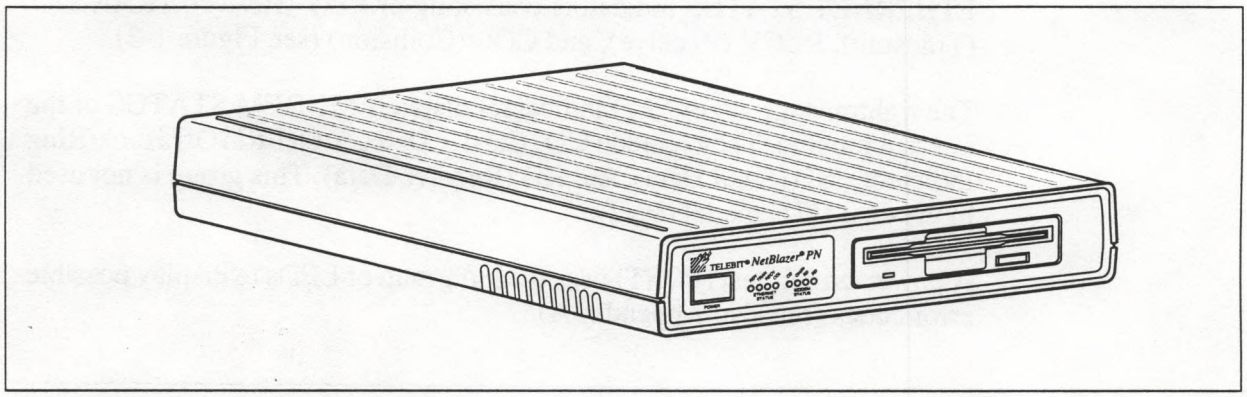


Figure 1-1. The NetBlazer PN1

The NetBlazer PN is ideally suited for installation in smaller remote sites as a dial-up router linking an Ethernet LAN to an enterprise-wide network. Its built-in synchronous port makes it a cost-effective Switched 56/Basic Rate ISDN router or an economical 56/64 Kbps router with built-in leased-line backup device.

Figure 1-2 illustrates the NetBlazer PN1 front panel. A rocker-type power switch is located on the far left. A standard 1.44-Mbyte 3.5-inch floppy diskette drive is located on the right.

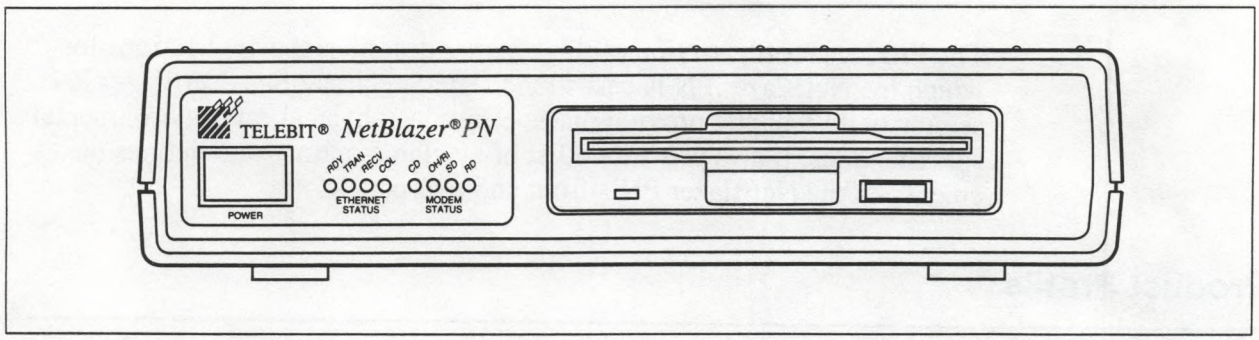


Figure 1-2. NetBlazer PN1 Front View

The LED indicators are arranged in two groups of four (the PN2 does not have the modem indicators). From left to right in the leftmost group are the ETHERNET STATUS indicators consisting of RDY (Ready), TRAN (Transmit), RECV (Receive), and COL (Collision) (see Figure 1-3).

The rightmost group of LED indicators displays MODEM STATUS of the internal modem. They include CD (Carrier Detect), OH/RI (Off Hook/Ring Indicator), SD (Send Data), and RD (Receive Data). This group is not used in the dual DTE model (PN2).

A power-on self test (POST) uses the left group of LEDs to display possible error codes (see also Appendix A).

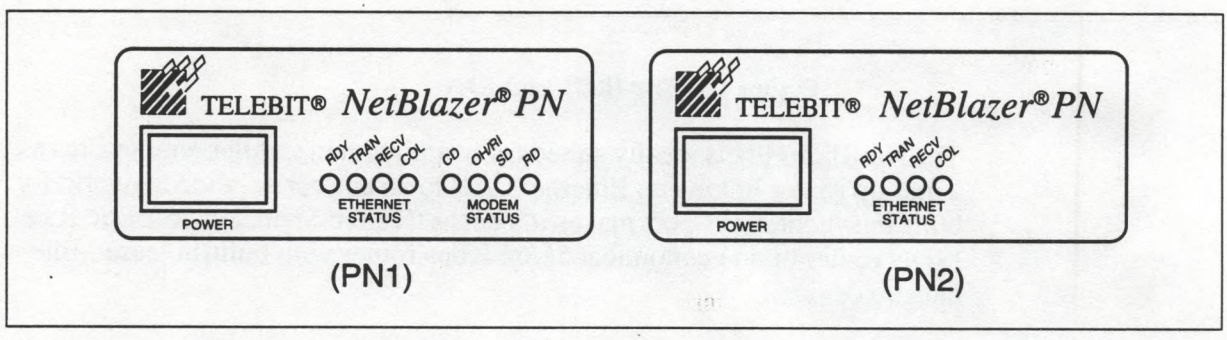


Figure 1-3. NetBlazer PN LED Panels

Both the Model PN1 and PN2 are provided with an Ethernet port. This port can be switched to the desired media type: AUI (10 Base5), BNC (10 Base2), or UTP (10 BaseT). The Ethernet MAC Address number is provided on an ID tag on the rear panel of each unit.

Model PN1

Figure 1-4 illustrates the NetBlazer PN1 rear panel with the Ethernet ports on the right, one serial port in the middle, and the telephone line interface on the left.

The serial port is electrically compatible with RS-423. This port follows RS–232C standard pinouts and works with any compliant RS-232C or EIA 232D device. It is available for connection to an external modem or asynchronous terminal at speeds up to 115.2 Kbps. It also works with a data service unit/channel switching unit (DSU/CSU) supporting a synchronous protocol up to 128 Kbps, with clocking provided by the DSU/CSU.

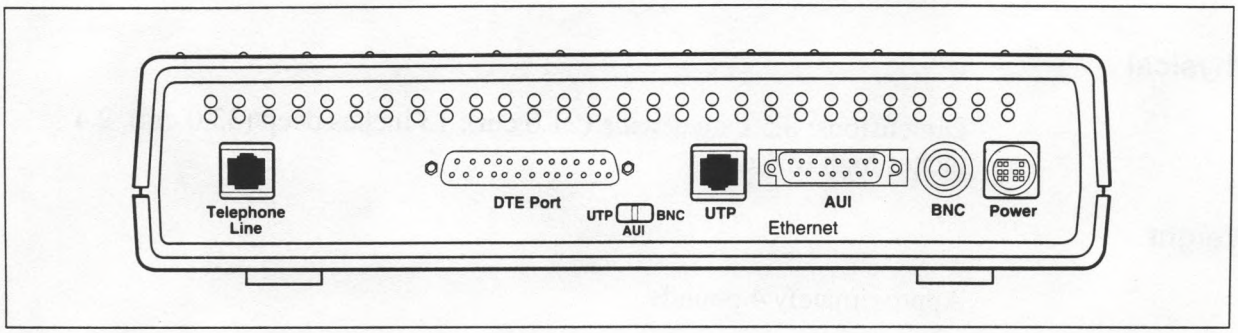


Figure 1-4. NetBlazer PN1 (with Modem) Rear Panel

Model PN2

Figure 1-5 illustrates the NetBlazer PN2 rear panel with the Ethernet ports on the right and the two serial ports on the left.

The serial ports are electrically compatible with RS-423. These ports follow RS-232C standard pinouts and work with any compliant RS-232C or EIA 232D device. They are available for connection to a modem or asynchronous terminal. Popular speeds up to 115.2 Kbps are supported. The DTE A port operates with a DSU/CSU supporting a synchronous protocol up to 128 Kbps, with clocking provided by the DSU/CSU.

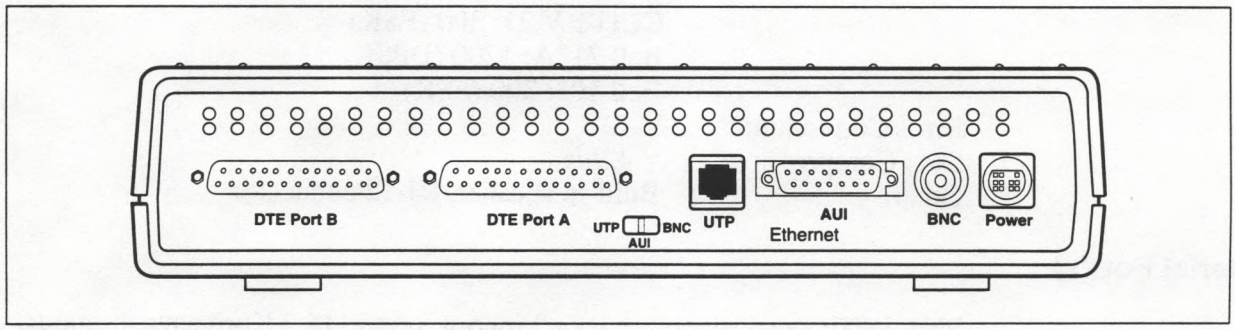


Figure 1-5. NetBlazer PN2 (Dual DTE) Rear Panel

Specifications–NetBlazer PN

Models

PN1-EFM: One serial DTE port, Ethernet port, floppy drive, and built-in modem.
PN2-EF: Two serial DTE ports, Ethernet port, and floppy drive.

Electrical

100–250 VAC, 50–60 Hz, universal autoranging power supply, 40 watts nominal, 90 watts maximum

Physical

Dimensions: 8.5 inches wide (21.6 cm), 13 inches deep (33.0 cm), 2.4 inches high (6.1 cm)

Weight

Approximately 4 pounds

Environmental

Operating Temperature: 10–50° C
Storage Temperature: -40–65° C
Humidity: 10–80% noncondensing

Internal Modem (PN1 only)

Modulation Capability:	CCITT V.32bis (V32FB-V42L only): 14,400 (TCM), 12,000 (TCM), 7200 (TCM) CCITT V.32: 9600 (TCM), 4800 (QAM) CCITT V.22bis: 2400 (QAM) CCITT V.22: 1200 (DPSK), 600 (DPSK) CCITT V.23: 1200 (FSK), 600 (FSK) CCITT V.21: 300 (FSK) Bell 212A: 1200 (DPSK) Bell 103: 300 (FSK)
Error Correction:	V.42
Data Compression:	V.42*bis*
Other:	Built-in speaker, RJ-12 connector

Serial Port(s)

PN1. DTE: synchronous or asynchronous, up to 115.2 Kbps asynchronous, and up to 128 Kbps synchronous with external clocking. Interface is RS-423 with RS-232C pinout convention. Connector type is a DB-25 male.

PN2. DTE A: same as above. DTE B: asynchronous only up to 115.2 Kbps. Interface is RS-423 with RS-232C pinout convention for both ports. Connector type is a DB-25 male.

Ethernet Port

Single Ethernet port, switch selectable to one of three media type interfaces: 10 Base5 (AUI), 10 BaseT (UTP), or 10 Base2 (thin Ethernet).

Accessories Furnished

PN1-EFM: One RJ-11 telephone line cable, one RS-232 straight-through (DB-25 male to DB-25 female) six-foot long cable (Telebit part number 14158-01), one null modem adapter (Telebit part number 14168-01), power supply, and AC line cord.

PN2-EF: Two RS-232 straight-through (DB-25 male to DB-25 female) six-foot long cables (Telebit part number 14158-01), one null modem adapter (Telebit part number 14168-01), power supply and AC line cord.

Preinstallation Planning 2

This chapter overviews the cables, equipment, and prerequisite information needed to install and cable the NetBlazer PN. Before starting the installation, read this chapter to make sure that you have all of the required equipment and information. This chapter also helps to familiarize you with what needs to be done to get the NetBlazer PN ready to use as quickly as possible.

General Planning

Before installing the NetBlazer PN, decide where it will be located, and make sure that you have the appropriate facilities and equipment needed to complete the installation.

When choosing a location for the NetBlazer PN, consider the AC outlets, telephone line, and Ethernet connection needed to support the NetBlazer PN. Avoid locating the unit in direct sunlight or near heating vents.

Ethernet Requirements

The NetBlazer PN comes with a built-in Ethernet adapter that can be connected to a local area network (LAN) using either the RJ-45 (10BaseT) connector, the BNC connector, or the 15-pin AUI connector. The BNC connector is used to tap into a thin Ethernet cable, whereas the AUI connector is used to connect the NetBlazer PN to the Ethernet through an external transceiver. The UTP connector is used with the RJ-45 plug for unshielded twisted-pair media.

You need to obtain any cables, hardware, and equipment required to connect the NetBlazer PN to your network. Appendix B provides pinouts for the Ethernet connectors.

Synchronous Interface Requirements

If you will be using the synchronous interface in your NetBlazer PN, you need to obtain a DSU or ISDN terminal adapter (TA) that supports an RS-232 interface.

To interface the NetBlazer PN to the DSU, use the straight-through RS-232 cable supplied (Telebit part number 14158-01). A wiring diagram of the RS-232C synchronous cable is illustrated in Figure 2-1.

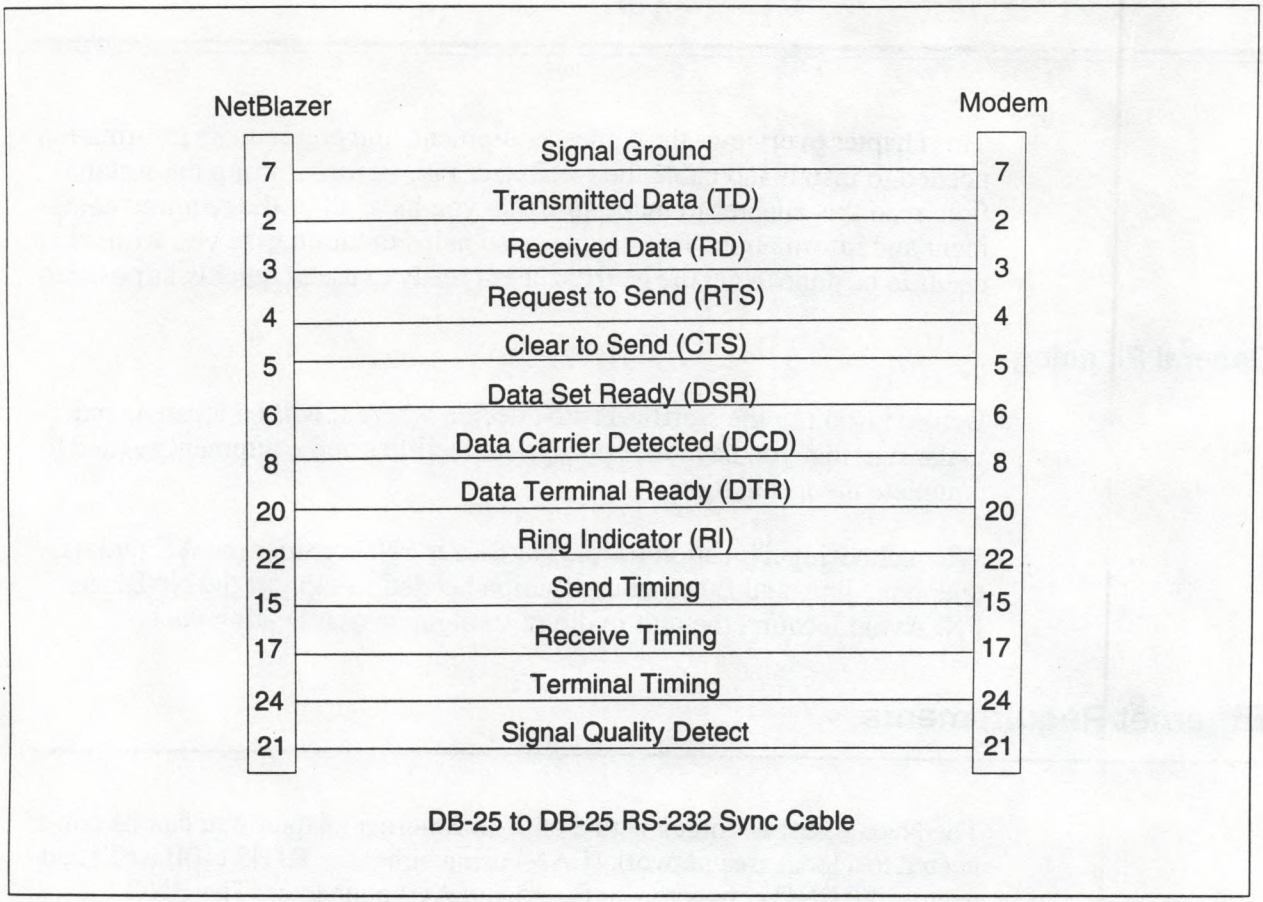


Figure 2-1. RS-232 Synchronous Cable Configuration

External Modem Requirements

Up to two standalone or rackmount external modems can be connected to the NetBlazer PN2, and one external modem can be connected to the PN1. Each standalone modem requires its own AC outlet and telephone line connection.

To connect a modem to either of the two standard asynchronous ports, you need a shielded RS-232 cable for each port. Use the straight-through RS-232 cable supplied (Telebit part number 14158-01). The NetBlazer PN asynchronous ports use the standard RS-232 signals shown in Figure 2-2.

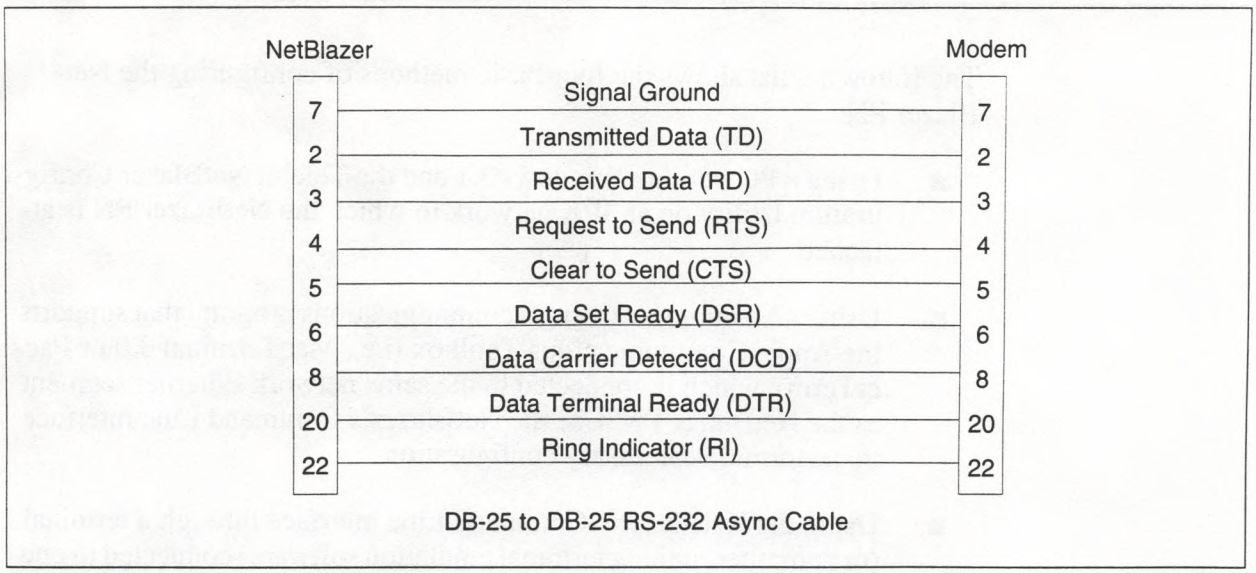


Figure 2-2. RS-232 Asynchronous Cable Configuration

The NetBlazer PN currently supports the external Telebit modems and firmware levels listed in Table 2-1.

Table 2-1. Supported Telebit Modems

Modem	Firmware Level	Firmware Level for AppleTalk ARA Service
WorldBlazer SA or RM	LA7.00 or later	LA7.03 or later
T3000 SA or RM	LA5.00 or later	LA7.03 or later
T2500 SA or RM	GE6.01, GF7.00, or later	
T2000 SA or RM	BC5.00 or later	
T1600 SA	LA5.00 or later	LA7.03 or later
T1500 SA	GE6.01, GF7.00, or later	
T1000 SA	FA2.00 or later	
T1000 RM	FC2.00 or later	
TrailBlazer Plus SA or RM	BC7.00, GF7.00, or later	

If you have a Telebit modem that is not at the required firmware level, contact your Telebit Technical Support representative for information about getting a firmware upgrade.

The following list shows the four basic methods of configuring the NetBlazer PN:

- Using a PC running Windows 3.1 and the Telebit NetBlazer Configuration Utility on an IPX network to which the NetBlazer PN is attached
- Using a Macintosh running a communications program that supports the Apple Communications Toolbox (i.e., MacTerminal 3.0 or PacerTerm), which is connected to the same network Ethernet segment as the NetBlazer PN. Use the NetBlazer's Command Line interface to perform the necessary configuration
- Using the NetBlazer's Command Line interface through a terminal (or computer running terminal emulation software) connected to one of the NetBlazer's asynchronous ports
- Using a PC running DOS to directly edit the NetBlazer's STARTUP.CNF file to preconfigure the NetBlazer PN so that it can be reached from your network. Then log into the NetBlazer PN through a *telnet* (IP protocol only) session from any host on the network

Using the NetBlazer Configuration Utility

Telebit recommends that you use its NetBlazer Configuration Utility. This utility provides a menu-oriented user interface to the NetBlazer for fast and easy configuration over an IPX link.

Note: *The DOS PC used to run the NetBlazer Configuration Utility must be attached to the same Ethernet segment as the NetBlazer PN.*

Using the NetBlazer's AppleTalk Interface

The NetBlazer PN's factory defaults have the ADSP Server and AppleTalk protocol active on the Ethernet port. This enables you to perform NetBlazer PN configuration using a Macintosh running a communications software package such as MacTerminal or PacerTerm.

Using the NetBlazer's Command Line Interface

If you are unable to use the NetBlazer Configuration Utility or prefer the use the NetBlazer's command line interface, you need an administrator's workstation (at least temporarily) to configure the NetBlazer PN. This can be done using one of two approaches:

- Connect a video display terminal or PC with terminal emulator to DTE port A using the RS-232 null modem adapter supplied (Telebit part number 14168-01).
- Set up an on-site workstation and modem that can be used to dial into the NetBlazer PN through the public switched telephone network (PSTN).

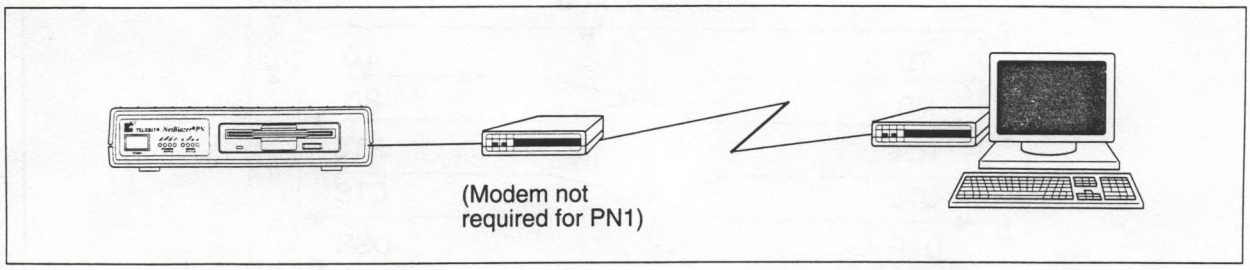


Figure 2-3. Dial-In Administrator's Workstation Configuration

Using DOS to Preconfigure the NetBlazer

To preconfigure the NetBlazer PN by editing the STARTUP.CNF file on the system diskette, you must have access to a system that supports 1.44-Mbyte, 3.5-inch DOS-formatted diskettes. Instructions for preconfiguring the NetBlazer PN system diskette are provided in the *NetBlazer Configuration Guide.*

Administrator's Workstation Requirements

To use a terminal (or computer with asynchronous communications software) as an administrator's control terminal, you need the RS-232 null modem adapter supplied (Telebit part number 14168-01) and cable (Telebit part number 14158-01). If you are constructing your own cable, Figure 2-4 shows the recommended null modem cable configuration for the NetBlazer PN. Your terminal (or computer) may require a different cable configuration. However, when choosing a null modem cable or adapter, observe the following requirements:

- The CTS signal to the NetBlazer PN must be held active high to allow the NetBlazer PN to transmit data.
- DSR and DCD must not be allowed to float.

You may also need an RS-232 gender changer to connect an RS-232 cable between two DTE devices.

A second choice, dialing into the NetBlazer PN from an on-site workstation, offers the advantage of testing the ability of the NetBlazer PN to process incoming calls from a remote site. However, this method requires an additional modem and telephone line for the administrator's workstation.

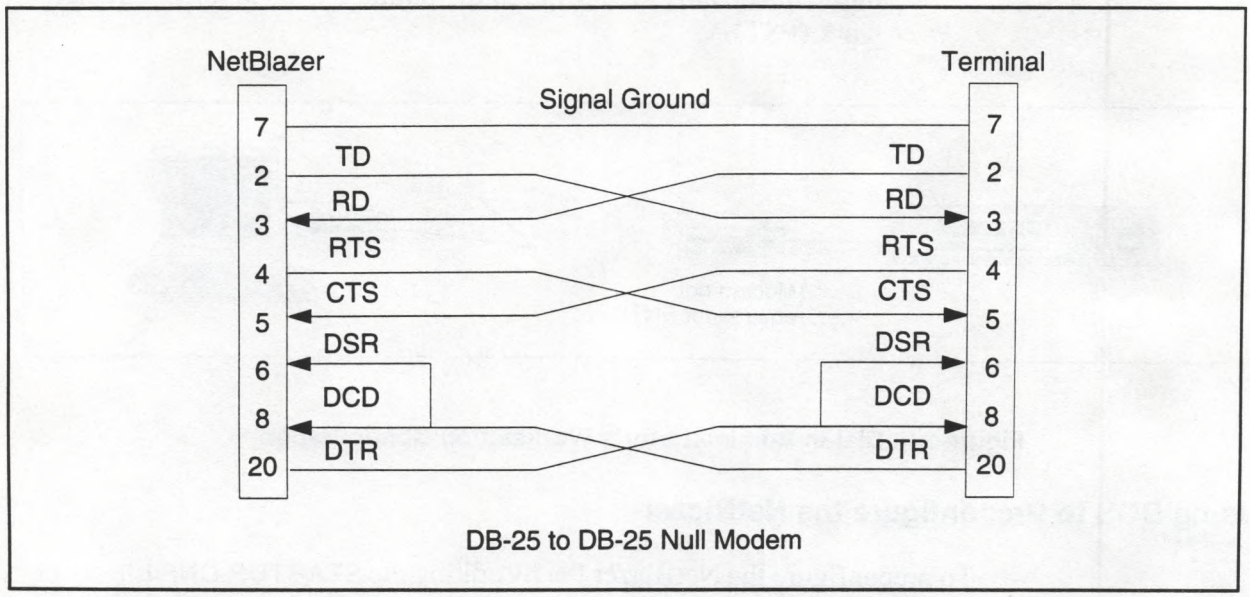


Figure 2-4. Null Modem RS-232 Cable Configurations

NetBlazer PN Installation 3

This chapter provides instructions for installing the NetBlazer PN and its associated components.

Telebit offers two basic NetBlazer PN configurations consisting of two serial ports or one serial port and a built-in V.32*bis* modem. Table 3-1 defines the ports on each model.

Table 3-1. NetBlazer PN Base Model Configurations

NetBlazer PN Model	Ethernet Port	Internal Modem	Serial Port A	Serial Port B
PN1	AUI, BNC, UTP	Single RJ-11	Sync/Async RS-423/ RS-232C	none
PN2	AUI, BNC, UTP	none	Sync/Async RS-423/ RS-232C	Async RS-423/ RS-232C

Connecting the Ethernet Port

The NetBlazer PN's Ethernet port can be connected to a LAN using the BNC connector for a thin Ethernet network, the 15-pin AUI connector when connecting to an external transceiver, or the RJ-45 connector for twisted pair. The location of the Ethernet media selector switch is shown in Figure 3-1.

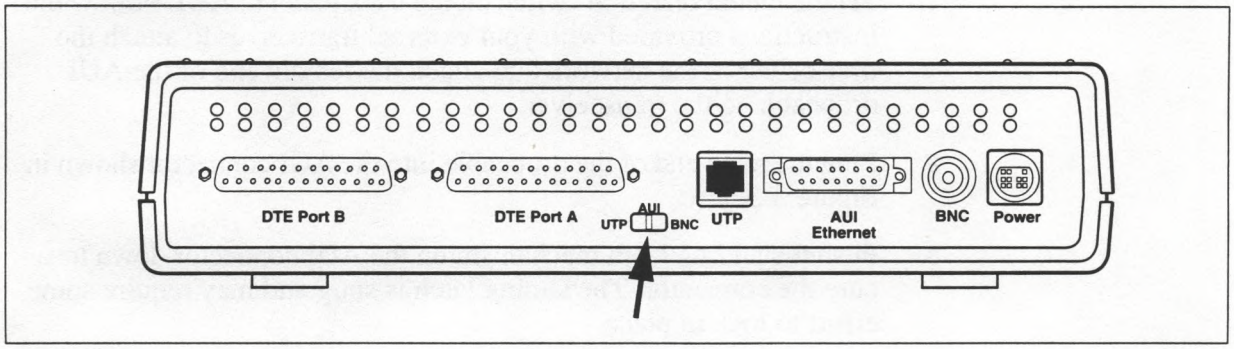


Figure 3-1. NetBlazer PN2 Ethernet Media Selector Switch

Connecting the NetBlazer PN to a Thin Ethernet (10Base2) Network

Perform the following steps to connect the NetBlazer PN to a thin Ethernet cable using a T connector (see Figure 3-2).

1. Set the Ethernet selector switch on the rear panel to BNC.
2. Attach the thin Ethernet cable to both ends of a T connector. If the NetBlazer PN is the last device on the cable, attach a 50-ohm terminator to one end of the connector. Neither side of the T connector should be left opened.
3. Plug the T connector into the BNC connector on the Ethernet board. Turn the T connector sleeve clockwise to lock in place.

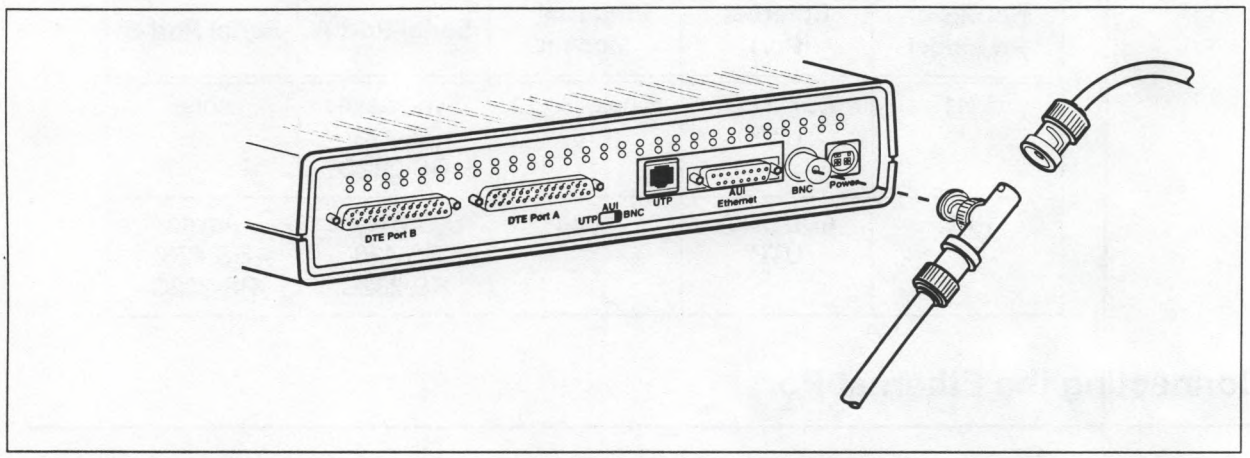


Figure 3-2. Thin Ethernet Connection

Connecting the NetBlazer PN to a Thick Ethernet (10Base5) Drop

To connect the NetBlazer PN to a thick Ethernet line using an external transceiver, perform the following steps:

1. Set the media selection switch on the back panel to AUI. Follow the instructions provided with your external transceiver to attach the transceiver to the network and attach the female end of the AUI dropcable to the transceiver.
2. Plug the male end of the dropcable into the AUI connector shown in Figure 3-3.
3. Push the sliding latch mechanism on the AUI connector down to secure the connector. The sliding latch is snug and may require some effort to lock in place.

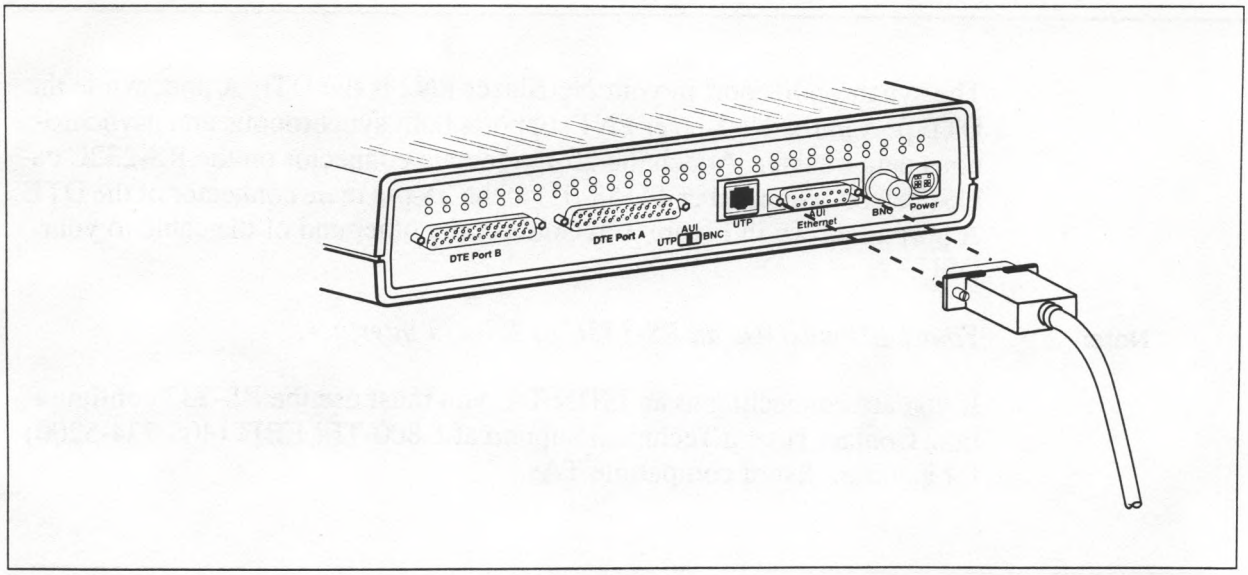


Figure 3-3. Ethernet AUI Connection

Connecting the NetBlazer PN to an RJ-45 Twisted Pair (10BaseT)

To use unshielded twisted pair media:

1. Set the Ethernet media selector switch on the rear panel to UTP.
2. Plug the RJ-45 cable connector into the RJ-45 socket on the Ethernet board as shown in Figure 3-4. UTP pin-out information is provided in Appendix B.

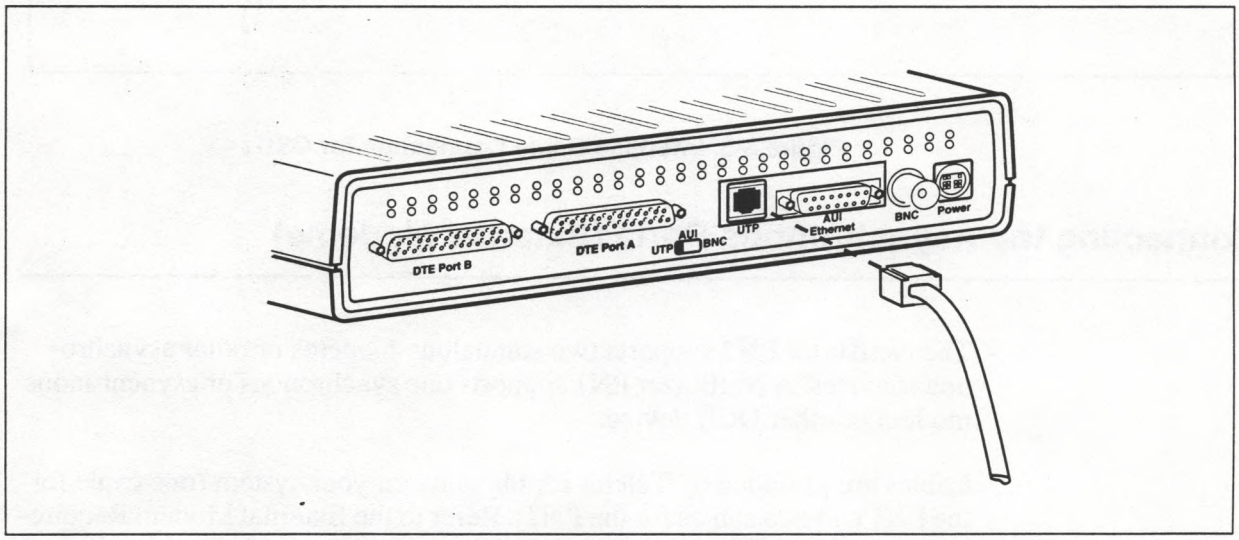


Figure 3-4. Ethernet RJ-45 Connection

Connecting the Synchronous Port

The synchronous port in your NetBlazer PN2 is the DTE A port, while the DTE port in the NetBlazer PN1 supports both synchronous and asynchronous data transfer. Attach the 25-pin female connector on the RS-232C cable (Telebit part number 14158-01) to the 25-pin male connector of the DTE A port as shown in Figure 3-5. Connect the other end of the cable to your DSU.

Note: *Your DSU must use an RS-232C or RS-423 interface.*

If you are connecting to an ISDN TA, you must use the RS-232 configuration. Contact Telebit Technical Support at 1-800-TELEBIT (408-734-5200) for a current list of compatible TAs.

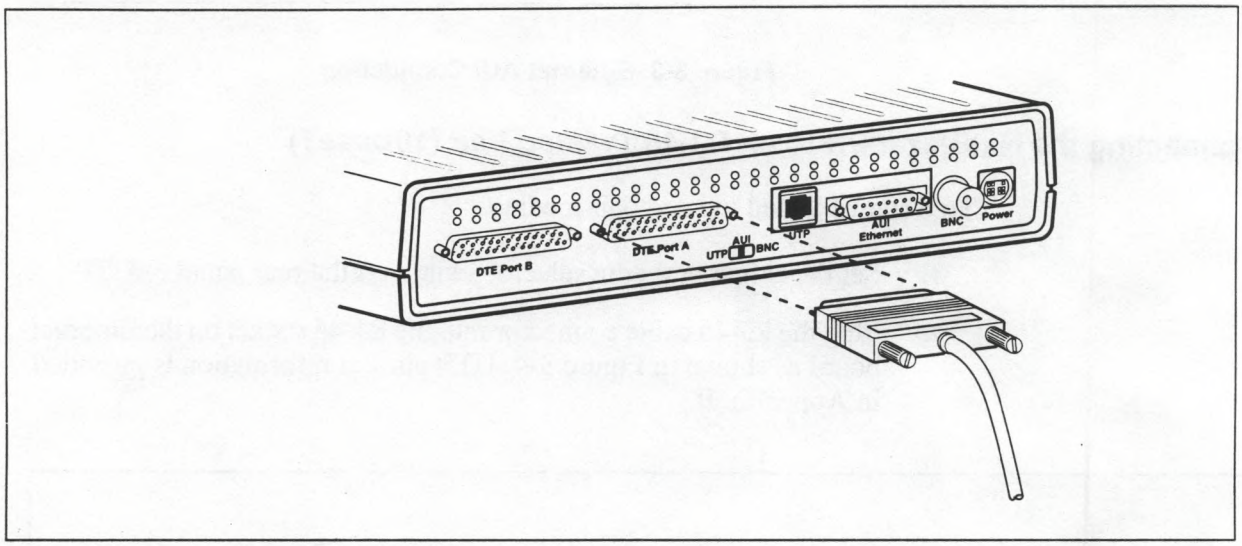


Figure 3-5. Interface Cable Connection for DSUs

Connecting the Asynchronous Ports (External Modems)

The NetBlazer PN2 supports two standalone modems or other asynchronous devices. A NetBlazer PN1 supports one synchronous or asynchronous modem or other DCE device.

Cables are provided by Telebit for the ports on your system (one cable for the PN1 and two cables for the PN2). Refer to the External Modem Requirements section in Chapter 2 for information on the appropriate cables. Pinout information is provided in Appendix B.

To connect a modem to either of the two standard asynchronous ports, attach the 25-pin female connector on your RS-232 cable to the appropriate connector shown in Figure 3-5. Attach the other end of the cable to the modem's RS-232 connector.

Refer to the manual supplied with your modem for further instructions on how to install and configure the modem.

Connecting the Internal Modem

To connect the NetBlazer PN1's internal modem, plug the telephone line into the RJ-11 connector, as shown in Figure 3-6.

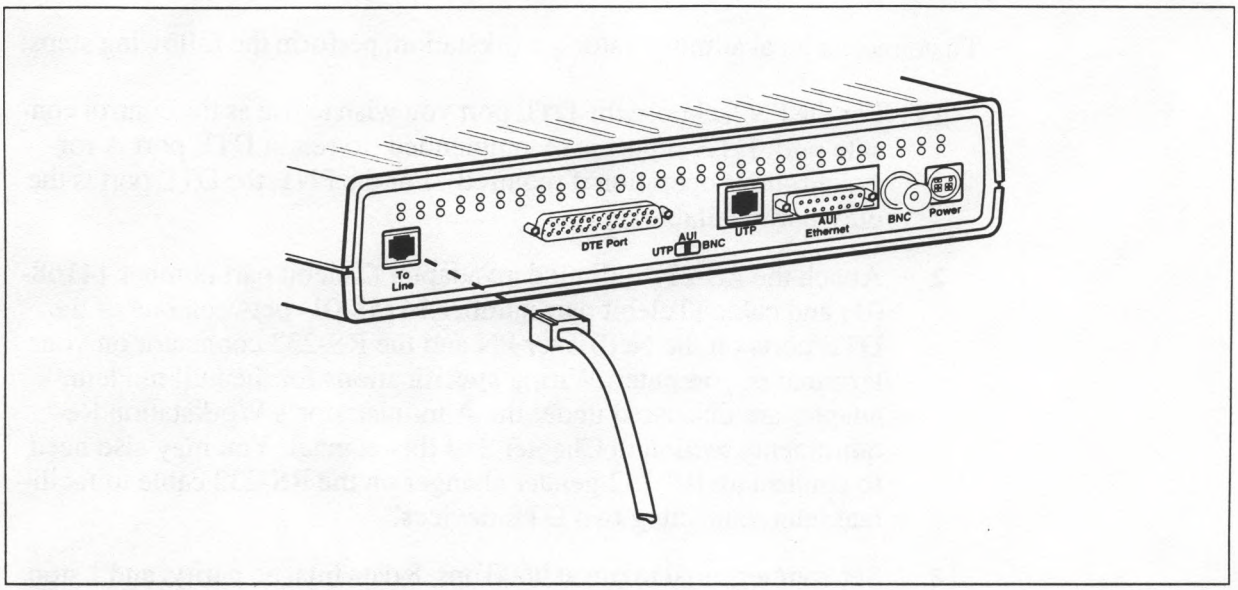


Figure 3-6. Connecting the Telephone Line to the NetBlazer PN1

Administrator's Workstation

If you have decided to edit the STARTUP.CNF file on the NetBlazer PN system diskette so that you can log into the NetBlazer PN from a host on your network using Telnet, you can skip this section. However, if you do not plan to preconfigure the NetBlazer PN system diskette, you must either set up an on-site dial-in workstation or connect an asynchronous terminal to one of the unused asynchronous ports using the supplied RS-232 null modem adapter (Telebit part number 14168-01).

Connecting a Dial-In Administrator's Workstation

To set up an on-site dial-in administrator's workstation, connect a terminal or computer with asynchronous communications software to your modem, and connect the modem to the telephone network. Refer to the manual supplied with your modem for detailed instructions on how to install and configure the modem.

For a PN2, connect a modem to DTE port B. Use a 25-pin to 25-pin modem cable (Telebit part number 14158-01).

For a PN1, connect the internal modem directly to the PSTN phone line using the RJ-11 telephone line cable supplied.

Connecting a Local Administrator's Workstation

To connect a local administrator's workstation, perform the following steps:

1. For the PN2, choose the DTE port you wish to use as the control console port. DTE B port is recommended (to retain DTE port A for synchronous operation if required). For the PN1, the DTE port is the only port available.
2. Attach the RS-232 null modem adapter (Telebit part number 14168-01) and cable (Telebit part number 14158-01) between one of the DTE ports on the NetBlazer PN and the RS-232 connector on your terminal or computer. Wiring specifications for the null modem adapter are discussed under the Administrator's Workstation Requirements section in Chapter 2 of this manual. You may also need to connect an RS-232 gender changer on the RS-232 cable to facilitate interconnecting two DTE devices.
3. Set your terminal to run at 9600 bps, 8 data bits, no parity, and 1 stop bit.

Connecting the AC Power Supply

Your NetBlazer PN is supplied with an autoranging universal power supply that automatically adapts itself to your line voltage. Connect the AC power cord supplied with your NetBlazer PN between the power cord connector on the power supply and an AC outlet. Connect the male DC power connector to the receptacle on the back of the NetBlazer PN, as shown in Figure 3-7.

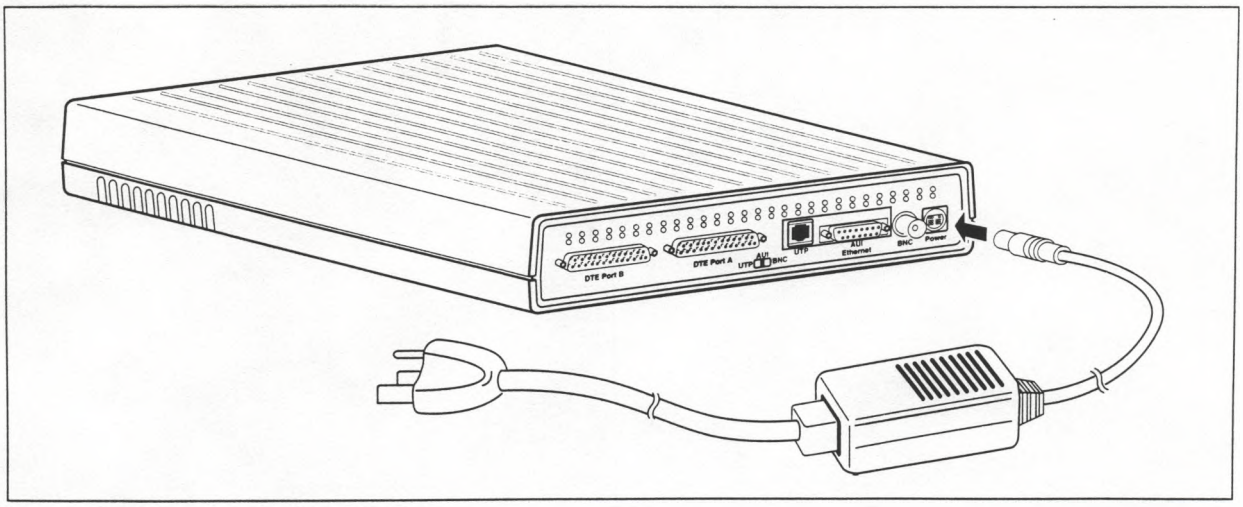


Figure 3-7. Connecting the NetBlazer PN Power Supply

NetBlazer PN POST Codes A

When the NetBlazer PN is first powered on, it performs two automatic processes:

- Power On Self Test (POST). This test consists of a series of specific hardware exercises that must successfully complete in turn. Passing this test indicates the NetBlazer PN is functioning normally.
- Booting. Loading the NetBlazer software from the floppy disk drive.

When the POST sequence has finished, all four LEDs in the group nearest the power switch flash on and off three times at a rate of once per second. At this point, the NetBlazer PN software begins loading from the floppy disk drive. During this time, the leftmost LED (RDY) blinks to indicate activity. Once software loading has finished, this LED stays on continually.

If an error is detected during POST, a stationary pattern is displayed on the Ethernet Status LEDs (see Figure A-1). Because the NetBlazer PN contains no user-serviceable components, this information is of greatest value to your Telebit Technical Support representative.

Note: *In the event of a POST failure, make a note of which LEDs are on before calling Telebit Technical Support at 1-800-TELEBIT. This information will help your support representative determine the most appropriate course of action to assist you.*

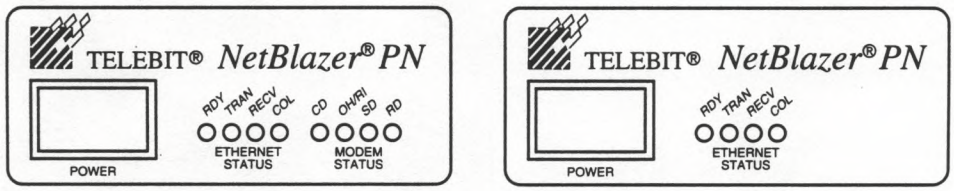


Figure A-1. NetBlazer PN LED Indicators

Interface Port Pinout Data B

The following pinout information is provided as a convenience to those who wish to fabricate their own cables and for general reference.

Ethernet Board Pinouts

DB-15 Connector

Pin	Description
1	Control in circuit shield (Shield)
2	Control in circuit A (Collision +)
3	Data out circuit A (Transmit +)
5	Data in circuit A (Receive +)
6	Voltage common (Power-Gnd)
9	Control in circuit B (Collision -)
10	Data out circuit B (Transmit -)
12	Data in circuit B (Receive -)
13	Voltage plus (Power +12V)
Shell	Protective ground

RJ-45 Socket

Pin	Description
1	Data Out (+)
2	Data Out (-)
3	Data In (+)
4	NC
5	NC
6	Data In (-)
7	NC
8	NC

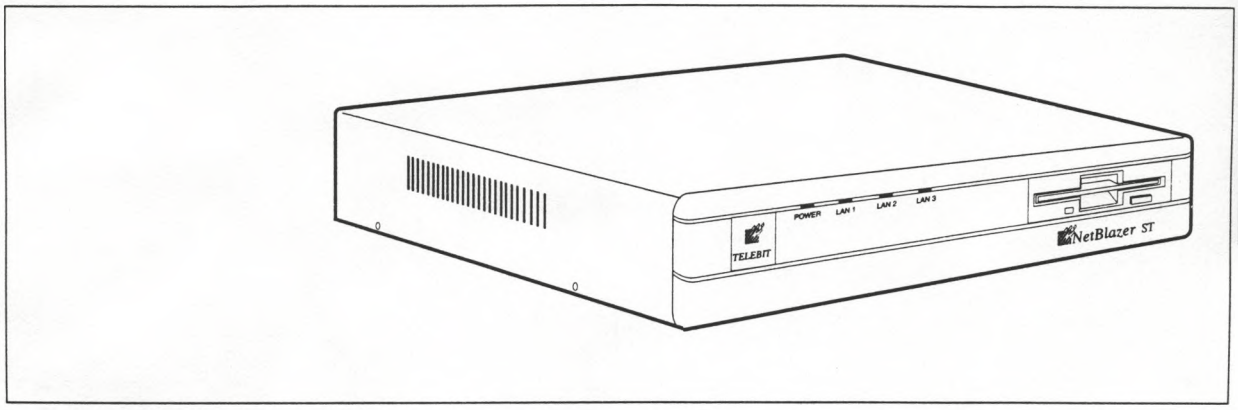
Synchronous Port Pinouts (DTE A)

The NetBlazer PN synchronous port is electrically compatible with RS-423 and follows RS-232C standard pinouts. It works with any compliant RS-232C or EIA-232D device supporting a synchronous protocol, with clocking up to 128 Kbps provided by the CSU/DSU.

Pin	Description
2	Transmit Data (TxD)
3	Receive Data (RxD)
4	Request to Send (RTS)
5	Clear to Send (CTS)
6	Data Set Ready (DSR)
7	Signal Ground
8	Data Carrier Detect (DCD)
15	Send Timing (TxC)
17	Receive Timing (RxC)
20	Data Terminal Ready (DTR)
21	Signal Quality Detect (SQD)
22	Ring Indicator (RI)
24	Terminal Timing (TT)

Asynchronous Port Pinouts (DTE Ports A and B in the PN2, DTE A in the PN1)

Pin	Description
2	Transmit Data (TxD)
3	Receive Data (RxD)
4	Request to Send (RTS)
5	Clear to Send (CTS)
6	Data Set Ready (DSR)
7	Signal Ground
8	Data Carrier Detect (DCD)
20	Data Terminal Ready (DTR)
22	Ring Indicator (RI)



NetBlazer ST

Installation Guide

90226-02

How to Use This Manual

This manual is a guide to installing the NetBlazer ST hardware. It is intended for use by the network administrator, technician, or engineer responsible for hardware installation. This guide covers all standard NetBlazer ST base models and the various option boards available.

Normally, options are specified when the initial order is made; the NetBlazer ST is preconfigured at the factory with any ordered options installed and preconfigured. However, options may also be purchased at any time after delivery or installation. This guide contains a section dedicated to field installation and preconfiguration of these options.

This manual consists of three chapters:

- Chapter 1, Introduction, provides an overview of the NetBlazer ST product, its features, and its applications. It also provides some basic product specifications.
- Chapter 2, Preinstallation Planning, reviews the information that you need to know before beginning the actual installation. Cable configurations and related information about the environment in which the NetBlazer ST will be operating are covered.
- Chapter 3, NetBlazer ST Options Installation, details the procedures required to change the factory default option settings or preconfigure and install new NetBlazer ST options.

Appendix A, Checking the NetBlazer ST Boot ROM Setup, provides information on the NetBlazer ST's boot ROM setup.

Related Documentation

Once the installation of the NetBlazer ST has been completed, you are ready to perform the software configuration. This procedure involves establishing the routes for the desired protocols you will use on the NetBlazer ST (and its options) and is covered in the *NetBlazer Configuration Guide*.

Generally, the Getting Started step-by-step configuration procedure, described in the *NetBlazer Configuration Guide*, must first be performed. Next, the desired protocols are configured. Beyond this, extensive customization of a broad range of operational parameters is available to those who wish to take advantage of the NetBlazer's rich capabilities. These facilities are also described in the *NetBlazer Configuration Guide*.

A complete listing of the NetBlazer's commands and comprehensive descriptions and examples of usage is contained in the *NetBlazer Command Reference* manual.

FCC Warning

This equipment generates and uses radio frequency energy, and if not installed and used in strict accordance with the instructions in this manual, may cause interference to radio and television reception. It has been tested and found to comply with the limits for a Class A computing device under Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference in a commercial installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the system on and off, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna
- Relocate the system with respect to the receiver
- Move the system away from the receiver
- Plug the system into a different outlet so that the system and receiver are on different branch circuits.

If necessary, consult your dealer or any experienced radio/television technician for additional suggestions. You may find a booklet prepared by the FCC entitled *How to Identify and Resolve Radio-TV Interference Problems* helpful in resolving any problems. This booklet is available from the U.S. Government Printing Office, Washington DC 20402, Stock Number 004-000-00345-4.

Table of Contents

1. Introduction

Product Profile 1-1
Specifications–NetBlazer ST 1-3
Electrical 1-3
Physical 1-3
Weight 1-3
Environmental 1-3
Options 1-3

2. Preinstallation Planning

General Planning 2-1
Ethernet Requirements 2-1
Token Ring Requirements 2-1
High-Speed Synchronous Interface Requirements 2-2
NS1 Single-Port Synchronous Board 2-2
SYN*xxx* Dual-Port Synchronous Board 2-4
Modem Requirements 2-4
ASYN8 Asynchronous Option 2-4
NM8 Asynchronous Option 2-4
Standard Asynchronous Ports (ASY00, ASY01, and Console: Chassis Mounted) 2-4
Compatibility 2-5
Configuration Methods and Considerations 2-6
Using the NetBlazer Configuration Utility 2-6
Using the NetBlazer's Command Line Interface 2-6
Using DOS to Preconfigure the NetBlazer ST 2-7
Administrator's Workstation Requirements 2-7

3. NetBlazer ST Options Installation

Nonstandard Configurations 3-1
Opening the NetBlazer ST Case 3-2
Configuring and Installing Option Boards 3-3
Removing the Power Supply 3-3
Installing (or Replacing) Option Boards and Power Supply 3-4

Appendix A, Checking the NetBlazer ST Boot ROM Setup

Figures

Closing the NetBlazer ST Case 3-4
Rackmount Adapter 3-5
Connect the AC Power Cord 3-5
Administrator's Workstation 3-6
Setting Up a Dial-In Administrator's Workstation 3-6
Connecting a Terminal Directly to an Asynchronous Port 3-6

Introduction 1

This manual provides instructions and related information required to install the NetBlazer ST. It is intended to be used by service personnel and qualified network administrators.

The Product Profile section of this chapter describes the applications for which the NetBlazer ST is best suited. It also defines the elements on the NetBlazer ST's front panel. The Specifications–NetBlazer ST section of this chapter provides basic electrical, physical, and environmental specifications. It also provides a list of available options and defines the elements on the NetBlazer ST's front and rear panels.

Product Profile

The NetBlazer ST is the slimline, desktop member of the NetBlazer family (see Figure 1-1). It provides a standard implementation of the NetBlazer software.

The NetBlazer ST is ideally suited for installation in smaller remote sites as a dial-up router linking one or two Ethernet or Token Ring local area networks (LANs) to an enterprise-wide network. Its ability to use synchronous ports makes it a cost-effective leased-line router, a leased-line backup device, or a router for switched digital services such as ISDN and Switched 56. It can also act as a central-site server for telecommuting applications that require up to 18 serial ports.

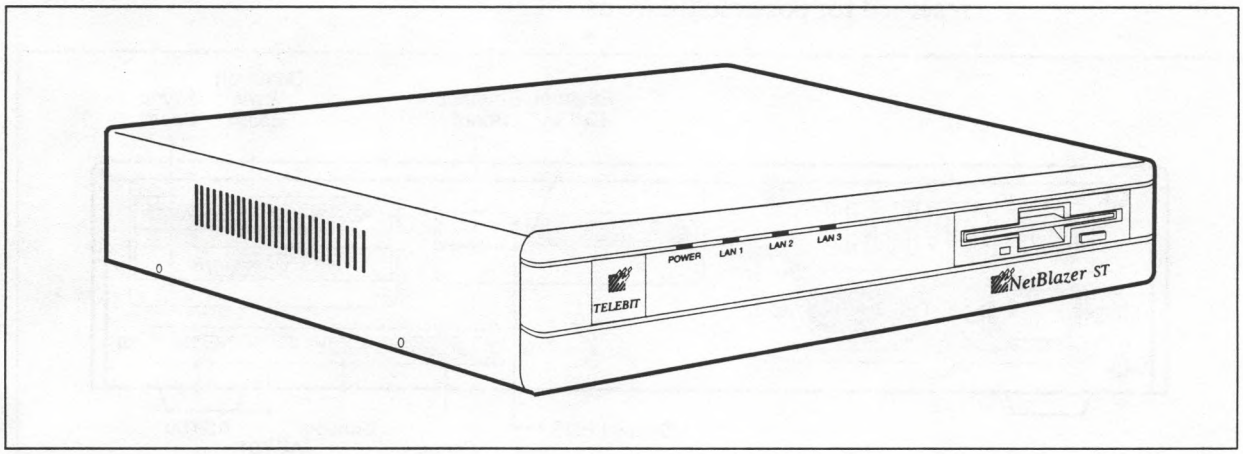


Figure 1-1. The NetBlazer ST

Figure 1-2 illustrates the NetBlazer ST front panel. The LED indicators from left to right are POWER, LAN1, LAN2, and LAN3. The POWER LED is on when AC power is applied to the NetBlazer ST. The LAN indicators light to show activity on the respective LAN channels (unused channels do not light).

A standard 1.44-Mbyte 3.5-inch floppy diskette drive is located on the right.

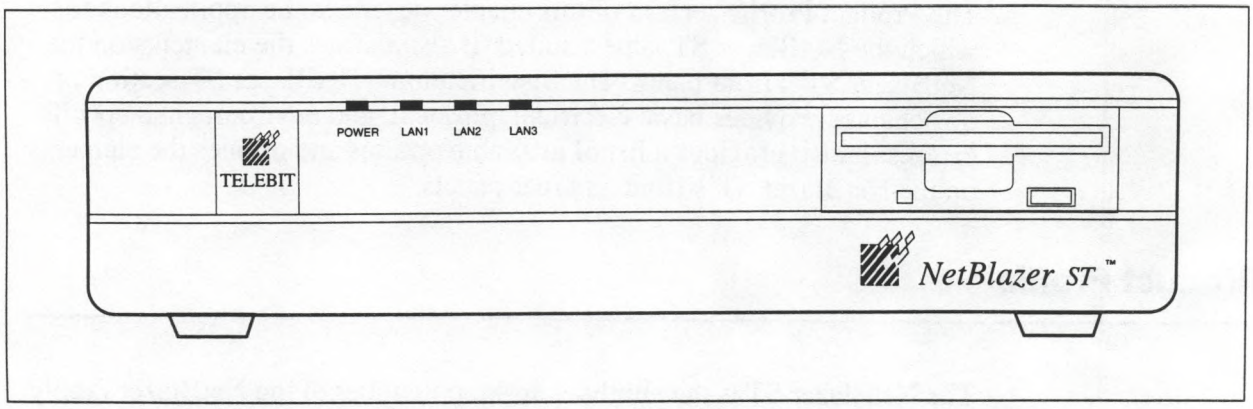


Figure 1-2. NetBlazer ST Front View

Figure 1-3 illustrates the NetBlazer ST rear panel with the Ethernet board installed in the left option board position and the dual-port synchronous and multiport asynchronous boards on the right.

Below the option slots are the chassis I/O ports. ASY00 and ASY01 are RS~232 9-pin ports available for connection to a modem or asynchronous terminal. The console port is also an RS-232 serial port for use with an asynchronous terminal operating at 9600 baud. The parallel printer port is reserved for possible future use.

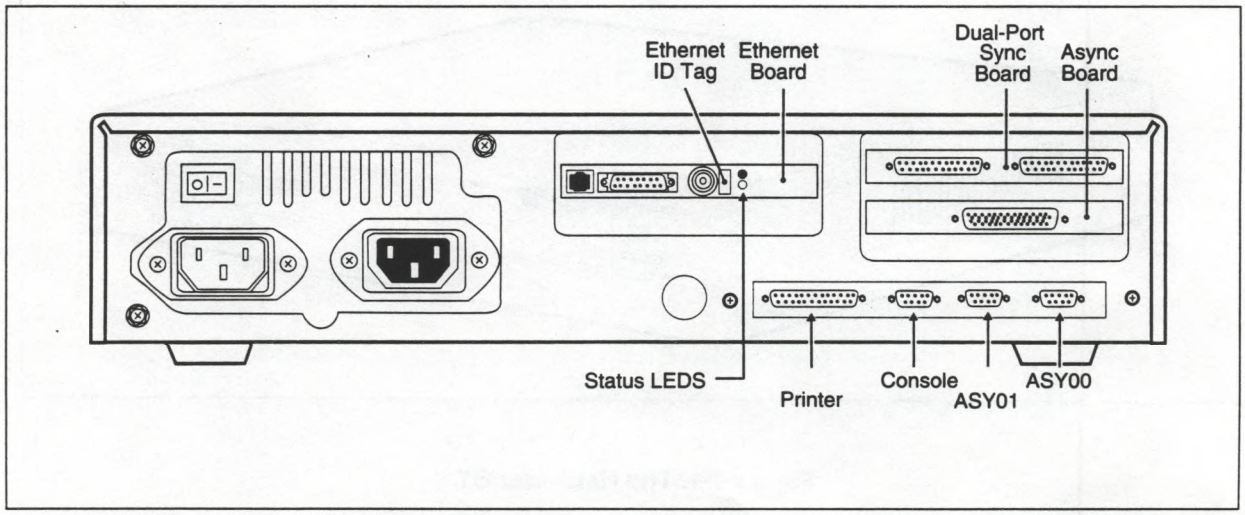


Figure 1-3. NetBlazer ST Rear Panel

Note the two LED indicators on the Ethernet board. The red LED indicates network receive status (it blinks while receiving data), and the green LED indicates twisted-pair network link status (off indicates a possible bad cable). The Ethernet MAC address number of the board is provided on an ID tag near the LEDs.

Specifications–NetBlazer ST

Electrical

90–260 VAC, 47–63 Hz, switch selectable or universal auto-ranging power supply, 100 watts

Physical

Dimensions: 15 inches wide x 15 inches deep x 3.25 inches high

Weight

Approximately 13 pounds, 9 ounces without option boards

Environmental

Operating Temperature: 10–40° C

Operating Humidity: 10–80% noncondensing

Options

Option Board Slots: Three

Option Boards:

- NE1 Ethernet
- NTR Token Ring
- NM8 Multiport Asynchronous
- ASYN8 Asynchronous with Modular Terminal Adapter (MTA)
- SYN*xxx* Dual-Port Synchronous

Up to three option boards may be installed in the NetBlazer ST.

A rackmount option is also available if you want to install the NetBlazer ST into a standard 19-inch rack.

Preinstallation Planning 2

This chapter overviews the cables, equipment, and prerequisite information you need to install and cable the NetBlazer ST. Before starting the installation, read this section to make sure that you have everything you need and to become familiar with what needs to be done to get your NetBlazer ST ready to use as quickly as possible.

General Planning

Before installing the NetBlazer ST, decide where it will be located, and make sure that you have the appropriate number of AC outlets, telephone lines, and Ethernet or Token Ring connections and equipment needed to complete the installation. Avoid locating the unit in direct sunlight or near heating vents.

Ethernet Requirements

The NetBlazer ST supports up to three Ethernet boards. Each Ethernet board can be connected to a LAN using either the RJ-45 (10BaseT) connector, the BNC connector, or the 15-pin AUI connector. The BNC connector is used to tap into a thin Ethernet cable, whereas the AUI connector is used to connect the NetBlazer ST to the Ethernet through an external transceiver.

You need to obtain any cables, hardware, and equipment required to connect the NetBlazer ST to your network. Pinouts for the Ethernet board connectors are provided in Appendix A of the *NetBlazer Option Boards Installation Guide*.

Token Ring Requirements

The NetBlazer ST supports up to three Token Ring boards. Each Token Ring board can be connected to a LAN using either the RJ-45 (UTP) connector or the 15-pin (STP) connector. The RJ-45 connector is used to connect to the ring with an unshielded twisted pair normally running at 4 Mbps, whereas the 15-pin shielded twisted-pair connector is used to connect rings running at 16 Mbps.

You need to obtain any cables, hardware, and equipment required to connect the NetBlazer ST to your network. Pinouts for the Token Ring board connectors are provided in Appendix A of the *NetBlazer Option Boards Installation Guide*.

NS1 Single-Port Synchronous Board

If you have the NS1 single-port synchronous interface board installed in your NetBlazer ST, you need to obtain a data service unit/channel switching unit (DSU/CSU) that supports a V.35, RS-422/RS-449, or an RS-232 interface.

The NS1 synchronous interface board is shipped from the factory configured for a DSU/CSU with a V.35 interface. Telebit provides the cable used to connect the NetBlazer ST to a DSU/CSU using a V.35 interface. This cable configuration is shown in Figure 2-1.

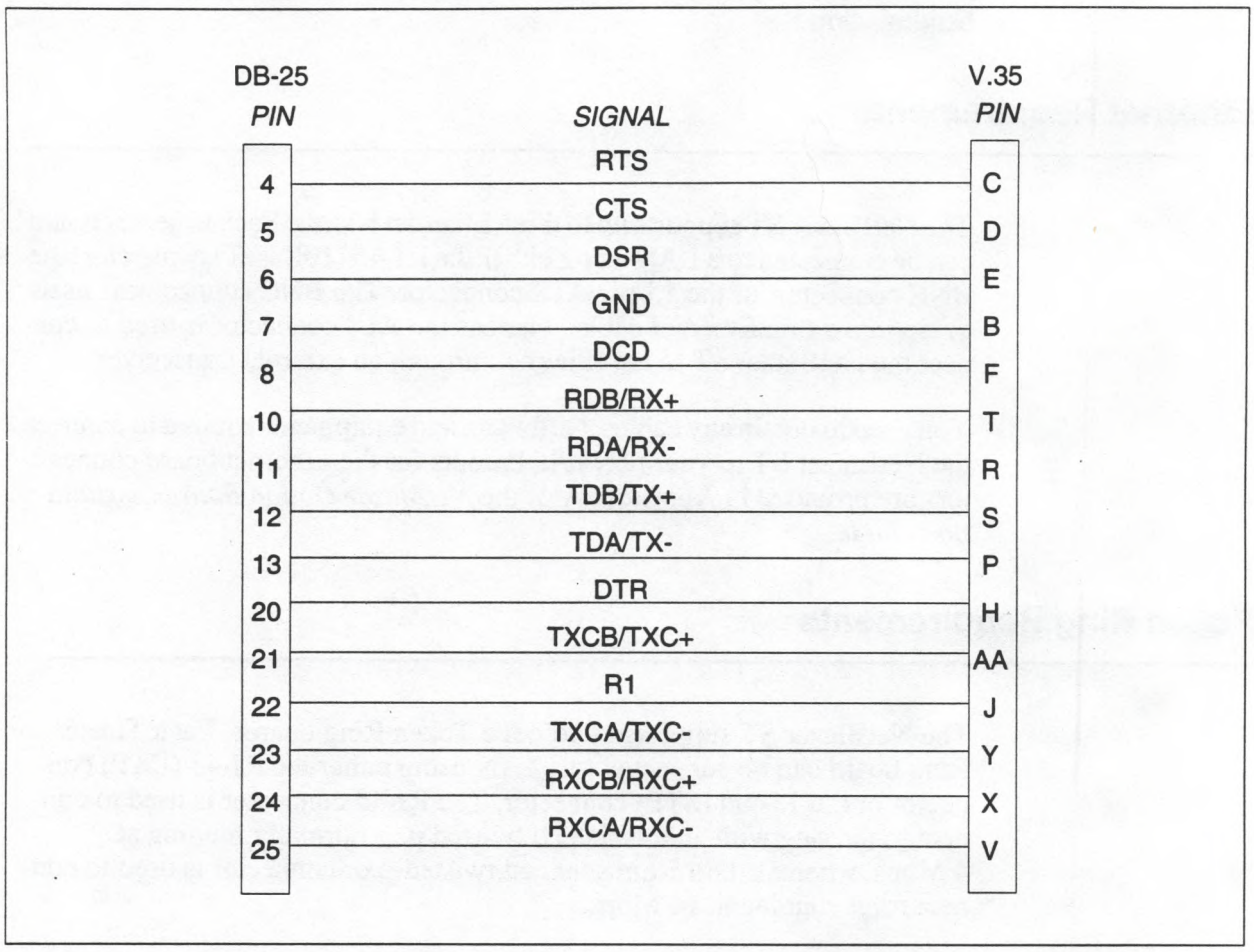


Figure 2-1. V.35 Cable Configuration

To connect the NetBlazer ST to a DSU/CSU using an RS-422/RS-449 or an RS-232 interface, you need to reconfigure the synchronous interface board as described in the *NetBlazer Option Boards Installation Guide* and obtain an appropriate cable.

An RS-422/RS-449 interface requires a special cable with a male DB-25 connector for the NetBlazer ST and a male DB-37 connector for the DSU/CSU. This cable should be configured as shown in Figure 2-2.

To use RS-232 interface to the DSU/CSU, you need a straight-through RS-232 cable with a male DB-25 connector on each end of the cable.

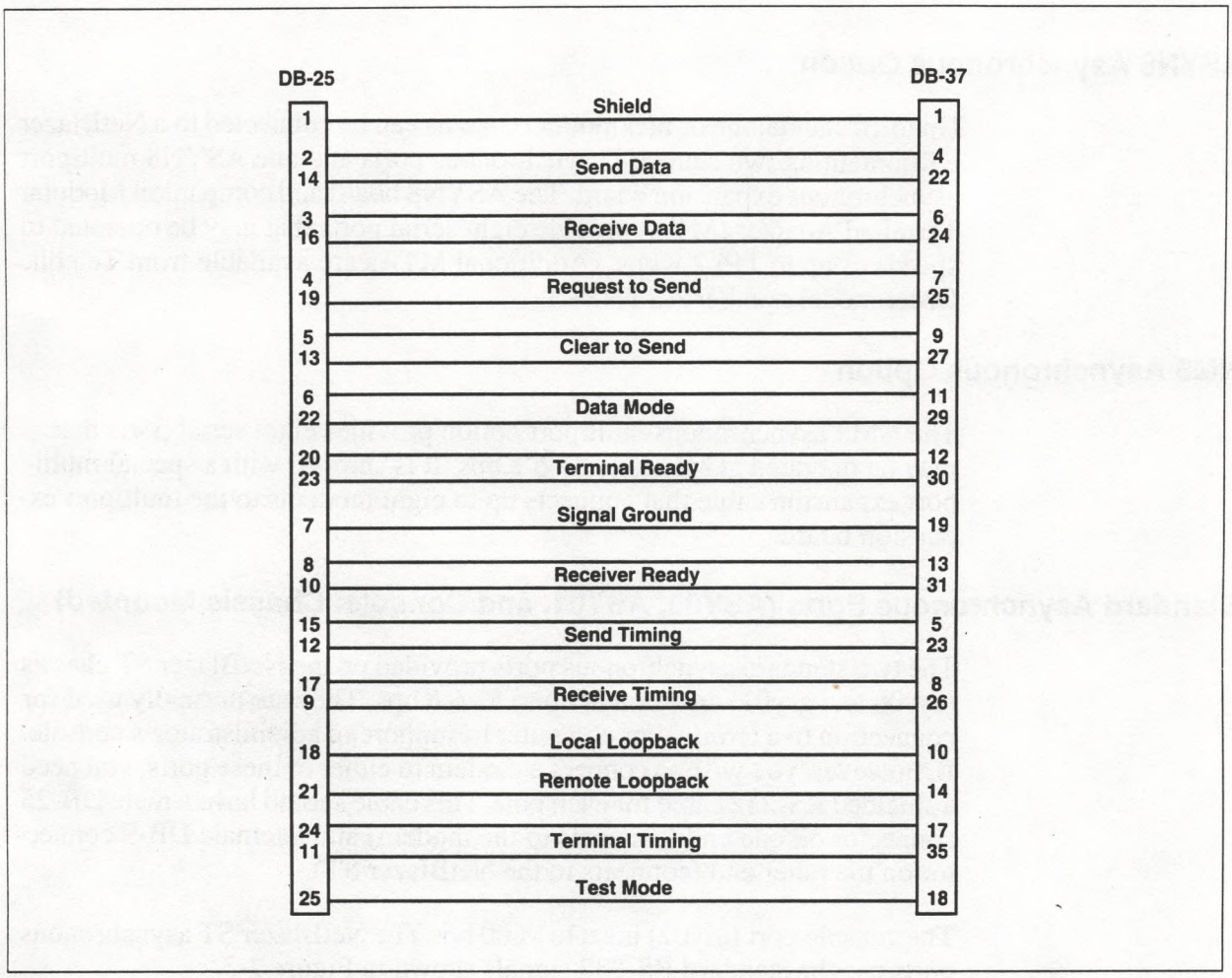


Figure 2-2. RS-422/449 Cable Configuration

SYN*xxx* Dual-Port Synchronous Board

If you have the model SYN*xxx* dual-port synchronous interface board installed in your NetBlazer ST, you have received the appropriate cables for the interface type specified when your initial order was placed. Note that if you want to use a T1/E1 line, you must attach this line to Port A. The B port can be used for connections up to 128 Kbps. Refer to the *NetBlazer Option Boards Installation Guide* for further information.

Modem Requirements

ASYN8 Asynchronous Option

Up to 10 standalone or rackmount modems can be connected to a NetBlazer ST containing two standard asynchronous ports and one ASYN8 multiport asynchronous expansion board. The ASYN8 board and companion Modular Terminal Adapter (MTA) provide eight serial ports that may be operated to speeds of up to 115.2 Kbps. (Additional MTAs are available from Telebit. Order model number ASYN8+.)

NM8 Asynchronous Option

The NM8 asynchronous multiport option provides eight serial ports that may be operated at speeds to 57.6 Kbps. It is shipped with a special multiport expansion cable that connects up to eight modems to the multiport expansion board.

Standard Asynchronous Ports (ASY00, ASY01, and Console: Chassis Mounted)

The two standard asynchronous ports provided on the NetBlazer ST chassis (asy00 and asy01) are rated at up to 57.6 Kbps. They are normally used for connection to a terminal or computer to support an administrator's console. If, however, you wish to connect a modem to either of these ports, you need a shielded RS-232 cable for each port. This cable should have a male DB-25 connector on one end (connects to the modem) and a female DB-9 connector on the other end (connects to the NetBlazer ST).

The console port (asy02) is set to 9600 bps.The NetBlazer ST asynchronous ports use the standard RS-232 signals shown in Figure 2-3.

Notes:

1. *For operation at the highest speeds, Telebit recommends using the ASYN8 or NM8 option ports instead of asy00 and asy01 ports.*
2. *Each standalone modem requires its own AC outlet and telephone line connection. The rackmount modem system, however, only requires one AC outlet and one RJ-23 telephone cable for each chassis.*

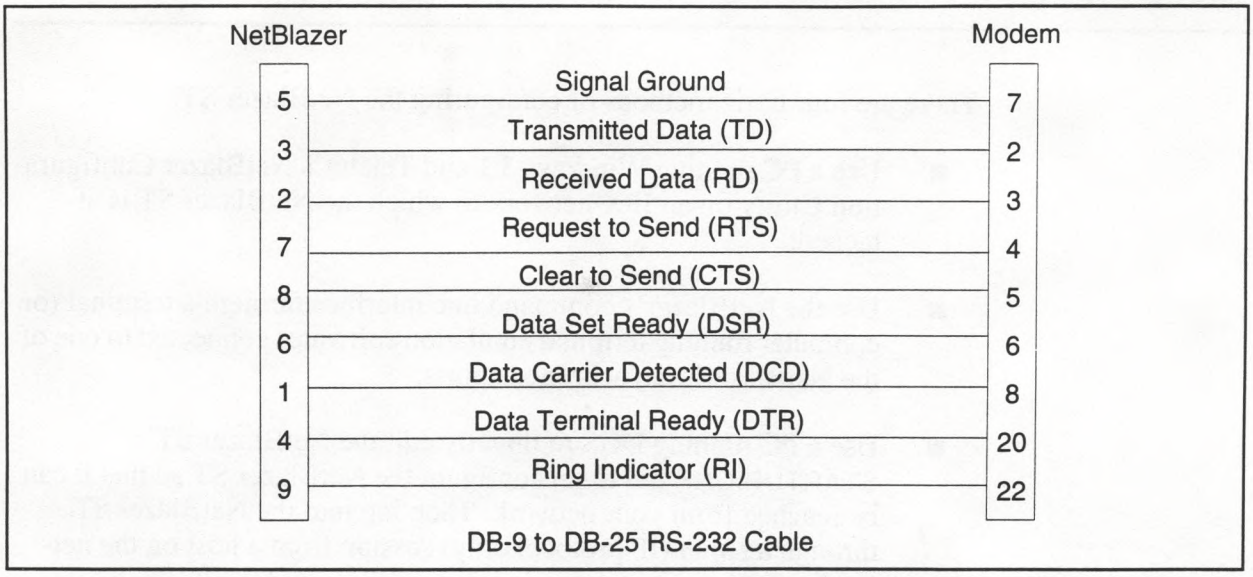


Figure 2-3. RS-232 Cable Configuration

Compatibility

The NetBlazer ST currently supports the Telebit modems and firmware levels listed in Table 2-1. If you have a Telebit modem that is not at the required firmware level, contact your Telebit Technical Support representative for information about getting a firmware upgrade.

Table 2-1. Supported Telebit Modems

Modem	Firmware Level	Firmware Level for AppleTalk ARA Service
QBlazer	MA1.01 or later	
WorldBlazer SA or RM	LA5.00 or later	LA7.03 or later
T3000 SA or RM	LA5.00 or later	LA7.03 or later
T2500 SA or RM	GE6.01, GE7.00, GF7.00, or later	
T2000 SA or RM	BC5.00 or later	
T1600 SA	LA5.00 or later	LA7.03 or later
T1500 SA	GE6.01, GF7.00, or later	
T1000 SA	FA2.00 or later	
T1000 RM	FC2.00 or later	
TrailBlazer Plus SA or RM	BC7.00, GF7.00, or later	

There are four basic methods of configuring the NetBlazer ST:

- Use a PC running Windows 3.1 and Telebit's NetBlazer Configuration Utility on an IPX network to which the NetBlazer ST is attached;
- Use the NetBlazer's command line interface through a terminal (or computer running terminal emulation software) connected to one of the NetBlazer's asynchronous ports;
- Use a PC running DOS to directly edit the NetBlazer ST's STARTUP.CNF file to preconfigure the NetBlazer ST so that it can be reached from your network. Then log into the NetBlazer ST through a *telnet* (IP protocol only) session from a host on the network;
- Use a Macintosh running a communications program that supports the Apple Communications Toolbox (i.e., MacTerminal 3.0 or PacerTerm), which is connected to the same network Ethernet segment as the NetBlazer ST. Use the NetBlazer's command line interface to perform the necessary configuration.

Using the NetBlazer Configuration Utility

Telebit recommends that you use its NetBlazer Configuration Utility. This utility provides a graphics-oriented user interface to the NetBlazer ST for fast and easy configuration of IP and IPX protocols over an IPX link.

Note: *The DOS PC used to run the NetBlazer Configuration Utility must be attached to the same Ethernet segment as the NetBlazer ST.*

Using the NetBlazer's Command Line Interface

If you are unable to use the NetBlazer Configuration Utility or prefer the use the NetBlazer's command line interface, you need an administrator's workstation (at least temporarily) to configure the NetBlazer ST (see Figure 2-4). This can be done using one of two approaches:

- Connect a video display terminal or computer directly to the console port or any unused asynchronous port (use an RS-232 null modem cable).
- Connect an on-site workstation to a modem and telephone line to dial into the NetBlazer ST through the public switched telephone network (PSTN).

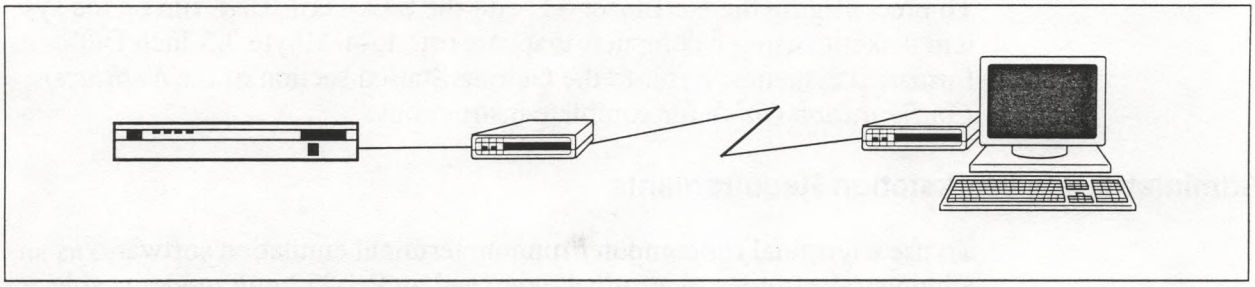


Figure 2-4. Dial-In Administrator's Workstation Configuration

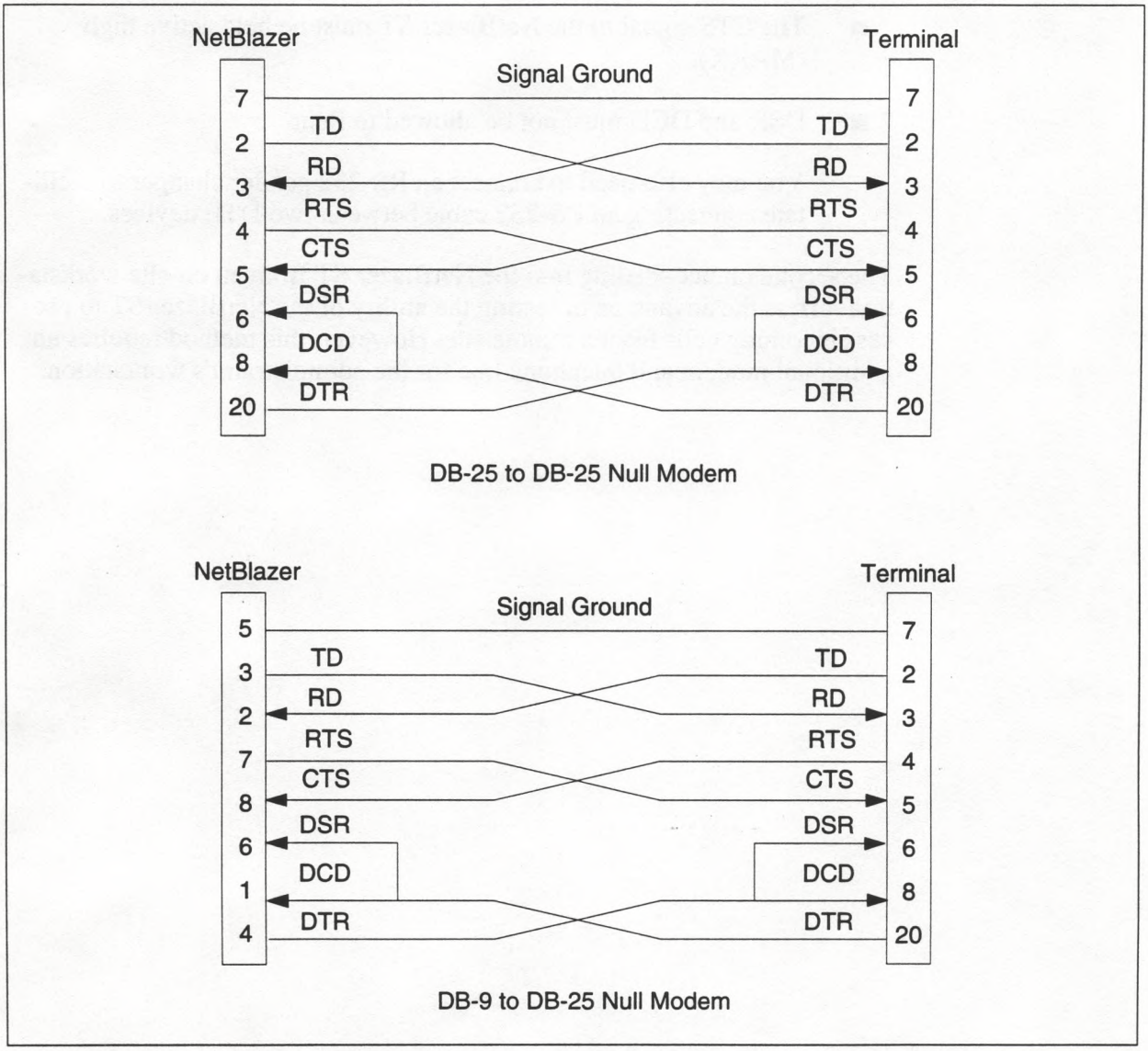


Figure 2-5. RS-232 Null Modem Cable Configurations

Using DOS to Preconfigure the NetBlazer ST

To preconfigure the NetBlazer ST, edit the STARTUP.CNF file on the system diskette, using a computer that supports 1.44-Mbyte 3.5-inch DOS-formatted diskettes. Refer to the Getting Started section of the *NetBlazer Configuration Guide* for complete instructions.

Administrator's Workstation Requirements

To use a terminal (or computer running terminal emulation software) as an administrator's control terminal, you need an RS-232 null modem cable (Telebit part number 12724-01) or adapter. If you are constructing your own cable, refer to Figure 2-5. Your terminal (or computer) may require a different cable adaptation. However, when using a null modem cable or an adapter, observe the following requirements:

- The CTS signal to the NetBlazer ST must be held active high (MARK).
- DSR and DCD must not be allowed to float.

  You may also need to connect an RS-232 gender changer to facilitate connecting an RS-232 cable between two DTE devices.

The second choice–dialing into the NetBlazer ST from an on-site workstation–offers the advantage of testing the ability of the NetBlazer ST to process incoming calls from a remote site. However, this method requires an additional modem and telephone line for the administrator's workstation.

NetBlazer ST Options Installation 3

This chapter provides instructions for installing the NetBlazer ST and its associated optional hardware components.

Telebit offers four basic NetBlazer ST configurations consisting of different option boards. Table 3-1 defines the option boards for each model.

Table 3-1. NetBlazer ST Base Model Configurations

NetBlazer ST Model	NE1 Ethernet Option Board*	Multiport Option Board (NM8)	Sync Option Board (NS1)**
NS2-1E	1	none	none
NS10-1E	1	1	none
NS2-1ES	1	none	1
NS10-1ES	1	1	1
Option board factory settings: * Coax interface (thin Ethernet) ** V.35 DSU/CSU interface			

Nonstandard Configurations

The four basic configurations in Table 3-1 cover most NetBlazer ST applications. If you are using one of these configurations, skip this chapter and proceed to the *NetBlazer Option Boards Installation Guide* for information on cabling the NetBlazer ST.

If your specific NetBlazer ST operating environment involves a different option configuration or LAN/DSU/CSU interface type other than identified above, you need to perform some degree of hardware preconfiguration. Examples include the following:

- **Ethernet Media Type.** The Ethernet board is preset for connection to a thin (coax) Ethernet cable through the BNC connector. If you are connecting the NetBlazer ST to an Ethernet network through an external transceiver, you must change jumpers on the Ethernet board to use the AUI connector. This is also true for the 10BaseT port.

- **Single-Port Synchronous Interface.** The high-speed synchronous interface board is shipped from the factory configured to connect to a DSU/CSU using a V.35 interface. If you connect the NetBlazer ST to a DSU/CSU with an RS-422/449 or RS-232 interface, the four jumper plugs on the board must be repositioned for the appropriate interface.

- **Multiple Dual-Port Synchronous Interface Boards.** If you plan to install more than one SYN*xxx* board, you need to set switch SW2 on one of the boards to assign the board's base I/O address.
- **Multiple Ethernet Boards.** Adding one or two Ethernet boards requires preconfiguring the IRQ level assigned to each board.
- **Token Ring.** Adding a Token Ring board (or boards) requires preconfiguring each board to the appropriate Token Ring speed and media type and setting the IRQ level assigned to each board.
- **Rackmounting.** The NetBlazer ST may be installed in an EIA standard 19-inch rack using the optional rack adapter.

If any of the above conditions *do* apply to your installation, the NetBlazer ST case must be opened, and the related hardware option must be preconfigured for your particular requirements. For these conditions, perform all of the following procedures that are applicable.

Opening the NetBlazer ST Case

Warning: *Make sure that the NetBlazer ST is not connected to an AC power outlet; then open the NetBlazer ST case by performing the following steps:*

1. Using a Phillips screwdriver, remove the two screws on each side of the NetBlazer ST top cover.
2. Slide the top cover backward about an inch, then lift the top cover off the NetBlazer ST (see Figure 3-1).

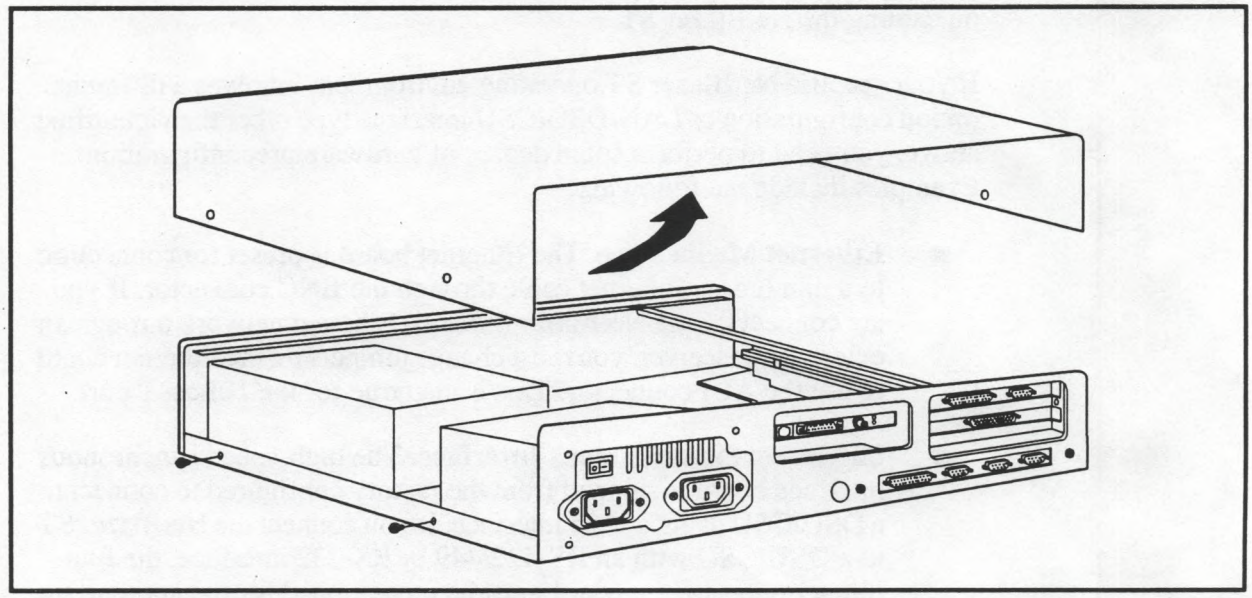


Figure 3-1. Removing the NetBlazer ST Cover

Refer to the *NetBlazer Option Boards Installation Guide* for details on configuring and installing option boards in the NetBlazer ST. Note that if you are installing an option board in the slot nearest the power supply, it may be necessary to unmount the power supply. If this is the case, refer to the following procedure.

Caution: *The option boards are sensitive to static electricity. Observe ESD handling precautions and discharge any static on your body by touching an unpainted surface of the NetBlazer's frame before inserting the board.*

Removing the Power Supply

Because of the NetBlazer ST's compact form factor, it may be necessary to unmount the power supply in order to remove the Ethernet board.

1. Remove the three screws on the rear panel that secure the power supply.
2. Gently lift the power supply out of its mounting tab on the bottom of the chassis and set down as far out of the chassis as lead length permits (see Figure 3-2).

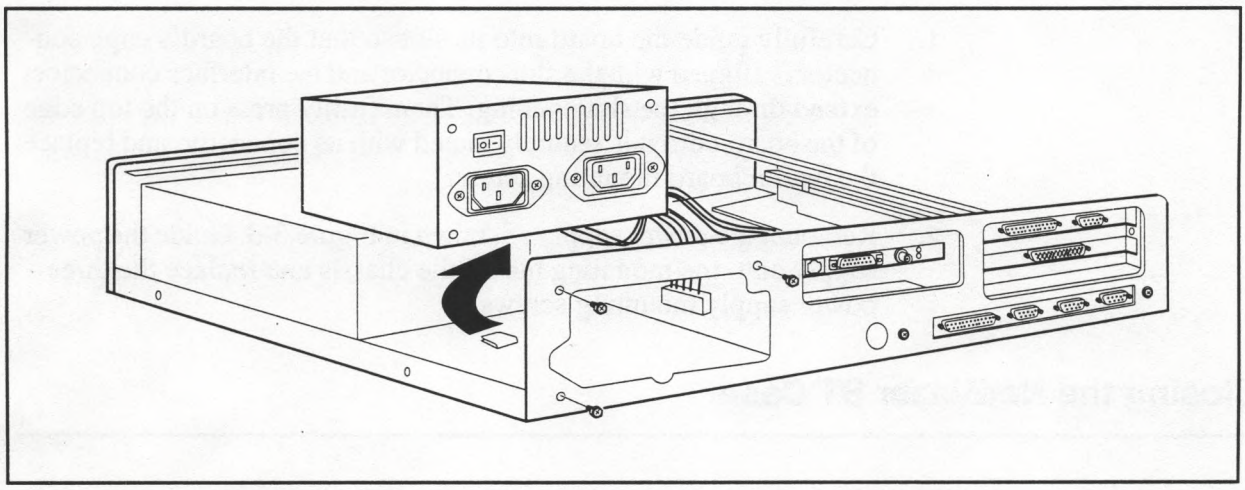


Figure 3-2. Removing the NetBlazer ST Power Supply

Installing (or Replacing) Option Boards and Power Supply

After completing all configuration changes, reinstall the option board.

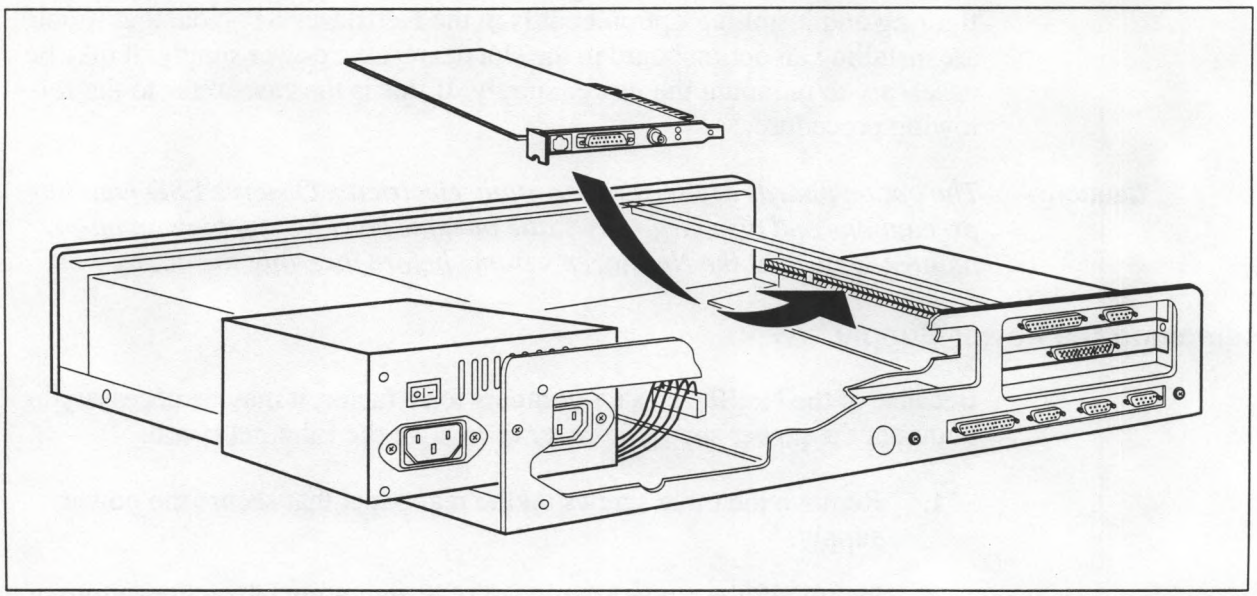


Figure 3-3. Replacing the Option Board and Power Supply

1. Carefully guide the board into its slot so that the board's edge connector is aligned with the slot connector and the interface connectors extend through the slot opening. Then, firmly press on the top edge of the board until it is securely mated with its connector, and replace the option board mounting screw.
2. Remount the power supply as shown in Figure 3-3. Guide the power supply onto the mounting tab on the chassis and replace the three power supply mounting screws.

Closing the NetBlazer ST Case

To close the NetBlazer ST case, perform the following steps:

1. Lower the top cover onto the NetBlazer ST so that the notches in the guide rails on the inside of the top cover align with the side edges of the front panel. Slide the top cover back into position.
2. If you do not plan to install the NetBlazer ST in a rack, replace the four cover mounting screws on the sides of the system. If you are rackmounting the unit, leave the screws out and go on to the next section.

Rackmount Adapter

If you have ordered the optional rackmount adapter, remove any packaging from the adapter and set the NetBlazer ST into the tray as shown in Figure 3-4.

Two sets of holes are provided to enable mounting the NetBlazer ST with or without its feet attached. Position the NetBlazer so the screw holes align, and replace the NetBlazer ST cover screws.

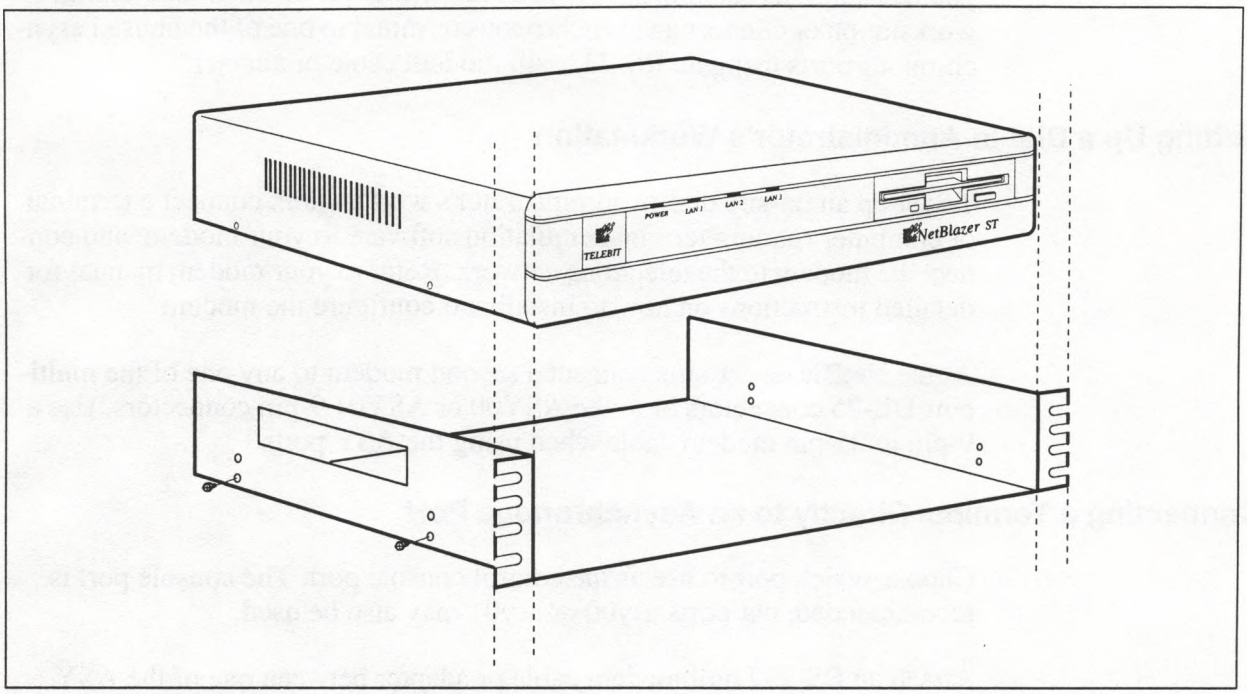


Figure 3-4. Installing the Rackmount Adapter

Once you have secured the NetBlazer ST into the adapter, the unit may be mounted in the rack. Be sure there are no obstructions to airflow on the side of the unit.

Connect the AC Power Cord

Connect the AC power cord supplied with your NetBlazer ST between the power cord connector on the back of the NetBlazer ST and an AC outlet.

Note: *The NetBlazer ST is equipped with a universal autosensing power supply; line voltage selection is performed automatically.*

If you have decided to:

- use the NetBlazer Configuration Utility (over an IPX link) or
- edit the STARTUP.CNF file on the NetBlazer ST system diskette so that you can log into the NetBlazer ST from a host on your network using telnet

you can skip this section. If not, you must either set up an on-site dial-in workstation or connect an asynchronous terminal to one of the unused asynchronous ports using an RS-232 null modem cable or adapter.

Setting Up a Dial-In Administrator's Workstation

To set up an on-site dial-in administrator's workstation, connect a terminal or computer running terminal emulation software to your modem, and connect the modem to the telephone network. Refer to your modem manual for detailed instructions on how to install and configure the modem.

At the NetBlazer ST site, connect a second modem to any one of the multiport DB-25 connectors or to the ASY00 or ASY01 9-pin connectors. Use a 9-pin to 25-pin modem cable when using the ASY ports.

Connecting a Terminal Directly to an Asynchronous Port

Choose which port to use as the control console port. The console port is recommended, but ports asy00 or asy01 may also be used.

Attach an RS-232 null modem cable or adapter between one of the ASY ports on the NetBlazer ST and the RS-232 connector on your terminal or computer (see Figure 3-5). Wiring specifications for the null modem cable or adapter are discussed under the Administrator's Workstation Requirements section in Chapter 2 of this manual. You may also need to connect an RS-232 gender changer on the RS-232 cable to interconnect two DTE devices.

Set your terminal or computer (running terminal emulation software) serial port to run at 9600 bps, 8 data bits, no parity, and 1 stop bit.

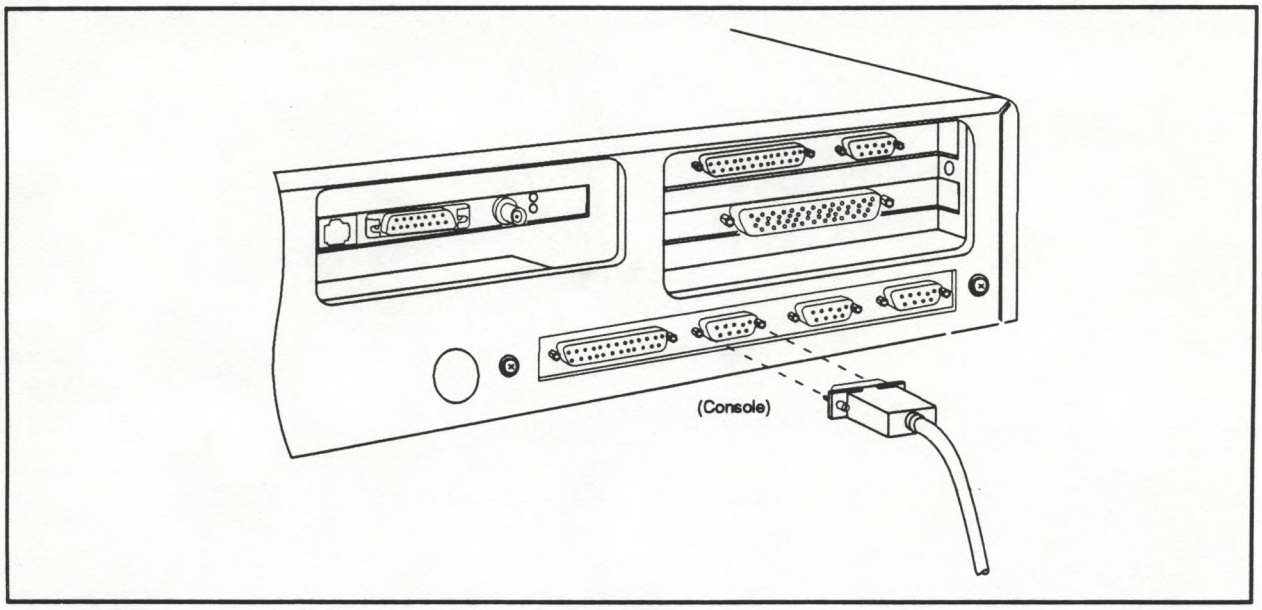


Figure 3-5. Connecting a Dial-In Administrator's Workstation to the NetBlazer ST

Checking the NetBlazer ST Boot ROM Setup

A

If the NetBlazer ST will not boot, there may be a problem with the boot ROM. Make sure that you have an asynchronous terminal (or computer running a terminal emulation program set to 9600 bps, 8 data bits, 1 stop bit, and no parity) (connected through a null modem cable) to the console port on the back of the NetBlazer ST and perform the following steps to check the ROM settings:

1. Remove the NetBlazer ST system diskette and then turn on the NetBlazer ST. The following information should be displayed on your terminal screen.

```
640K  Base Memory
2048K Total Memory
Non-Cache System

TELEBIT ROM version 2.00
Copyright (c) 1985-1992 Landmark Research Int'l Corp.
All rights reserved.

Press "B" for boot or "S" for setup
```

2. Enter **s** to view the current ROM settings.

```
T E L E B I T   S E T U P
Version 2.00
Copyright (c) 1985-1992 Landmark Research Int'l Corp.
ALL RIGHTS RESERVED

Current date: 1/21/92
Current time: 11:07:15
Diskette A: 1.44 Megabyte drive (3.5")
Diskette B: Not Installed
Hard Disk 0: Not Installed
Hard Disk 1: Not Installed
Base Memory: 640 KiloBytes
Extended Memory: 1,408 KiloBytes
Cache limited to 4 Megabytes
Primary display: Monochrome display (MDA)

("Yes" or <ENTER> will reboot system
Is this correct ("Yes", <ENTER>, "No", or <ESC>?
```

The drive and memory configuration settings displayed on your screen should match the settings shown above.

3. If the settings displayed on your screen are correct, enter **y**. Insert your working copy of the NetBlazer ST system diskette and press the Enter or Return key to reboot the NetBlazer ST. If the system still does not boot, contact your technical support representative.

If the settings displayed are not correct, enter **n** to begin the setup dialog, which allows you to make changes to the current setup options.

```
Current Date: 02/21/1992
Current Time: 13:26:35

Is this correct ("Yes", <ENTER>, "No", or <ESC>?
```

4. If the current date and time displayed are correct, press the Enter or Return key to continue. Otherwise, enter **no** and press the Enter or Return key. Enter today's date in the format shown (be sure to use four numeric characters for the year).

```
Current time: 14:46:36

Type new time (HH:MM:SS) or <ENTER> to accept?
```

5. If the current time displayed is correct, press the Enter or Return key to continue. Otherwise, enter the time in the format shown. Note that the NetBlazer uses a 24-hour clock; e.g., 1:00 p.m. is entered as 13:00:00, and 11:59 p.m. is entered as 23:59:00.

```
Current date: 02/21/1992
Current time: 15:01:50

Is this correct ("Yes", <ENTER>, "No", or <ESC>)? yes
```

6. Verify that the current date and time are correct by entering **yes** to the above prompt.

```
Base Memory: 640 Kilobytes


Is this correct ("Yes", <ENTER>, "No", or <ESC>)?
```

7. The NetBlazer ST is shipped with the maximum amount of base memory of 640 Kbytes. If the base memory displayed is not equal to 640 Kbytes, answer **no** to the above prompt and enter **640** when prompted for the base RAM size in kilobytes. Normally this should not need to be changed.

```
Extended Memory: 1,408 Kilobytes
Cache limited to 4 Megabytes

Is this correct ("Yes", <ENTER>, "No", or <ESC>)?
```

8. The standard 2-Mbyte NetBlazer ST is shipped with 1,408 Kbytes of extended memory. If the extended memory displayed is not equal to 1,408 Kbytes, answer **no** to the above prompt and enter **1,408** when prompted for the extended RAM size in kilobytes.

   A 4-Mbyte NetBlazer ST has 3,456 Kbytes of extended memory. Enter this value if you have upgraded to 4 Mbytes.

```
Limit caching to 4 Megabytes?
Is this correct ("Yes", <ENTER>, "No", or <ESC>)?
```

9. The NetBlazer ST does not support cache memory. Enter **yes** to the above prompt to proceed.

```
Primary display: Monochrome display (MDA)

Is this correct ("Yes", <ENTER>, "No", or <ESC>)?yes
```

10. Because the NetBlazer ST does not use an internal video display board, this setting is insignificant. Enter **yes** to the above prompt to proceed.

```
Diskette A: 1.44 Megabyte drive (3.5")
Diskette B: Not Installed

Is this correct ("Yes", <ENTER>, "No", or <ESC>)?yes
```

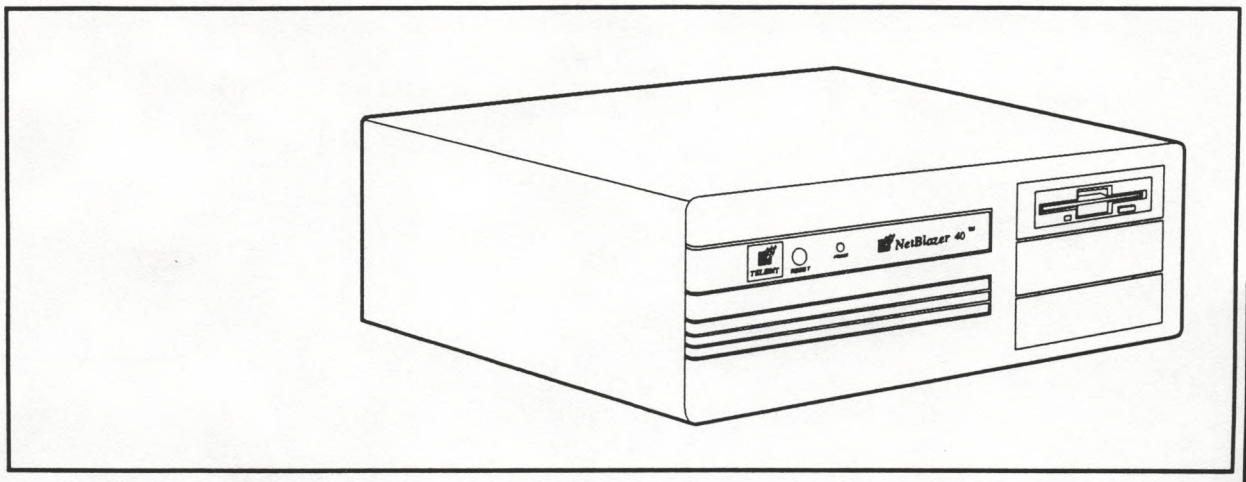
11. The NetBlazer ST is shipped with one 3.5-inch 1.44-Mbyte diskette. If the diskette information displayed is incorrect, answer **no** to the above prompt and enter **4** to select a 1.44-Mbyte drive when prompted for the type for drive A. Enter **0** for drive B.

```
Hard Disk 0: Not Installed
Hard Disk 1: Not Installed

Is this correct ("Yes", <ENTER>, "No", or <ESC>)?yes
```

12. The NetBlazer ST system does support a hard disk drive. If the internal hard disk information displayed is incorrect, answer **no** to the above prompt. Enter **0** when prompted for the number of hard disk drives.

```
T E L E B I T   S E T U P
Version 2.00
Copyright (c) 1985-1992 Landmark Research Int'l Corp.
ALL RIGHTS RESERVED

Current date: 02/21/1992
Current time: 15:16:30
Diskette A: 1.44 Megabyte drive (3.5")
Diskette B: Not Installed
Hard Disk 0: Not Installed
Hard Disk 1: Not Installed
Base Memory: 640 Kilobytes
Extended Memory: 1,408 Kilobytes
Cache limited to 4 Megabytes
Primary display: Monochrome display (MDA)

("Yes" or <ENTER> will reboot system)
Is this correct ("Yes", <ENTER>, "No", or <ESC>)? yes
```

13. Confirm that the displayed settings are correct by entering **y** to the above prompt. Then, insert your working copy of the NetBlazer ST system diskette, and press the Enter or Return key to reboot the system. If the system still does not boot, contact your technical support representative.



NetBlazer 40

Installation Guide

90225-02

How to Use This Manual

This manual is a guide to installing the NetBlazer 40 hardware. It is intended to be used by the network administrator or technician/engineer responsible for hardware installation. This guide covers the standard NetBlazer 40 base modes and the various option boards available.

Normally the NetBlazer 40 is shipped from the factory without any options installed. Options specified in the initial order must be configured and installed as required. However, options may also be purchased at any time after delivery or installation.

This manual consists of three chapters:

- Chapter 1, Introduction, provides an overview of the NetBlazer 40 product, its features, and its applications. It also provides some basic product specifications.
- Chapter 1, Preinstallation Planning, reviews the cable configurations and related information about the environment in which the NetBlazer 40 will be operating that you need to know before beginning the actual installation.
- Chapter 3, NetBlazer 40 Options Installation, details the procedures required to change the factory default option settings or preconfigure and install new NetBlazer 40 options.

Related Documentation

Once the installation of the NetBlazer 40 has been completed, you are ready to perform the software configuration. This procedure involves establishing the routes for the desired protocols you will use on the NetBlazer 40 (and its options) and is covered in the *NetBlazer Configuration Guide*.

Generally, the Getting Started step-by-step configuration procedure, described in the *NetBlazer Configuration Guide*, is adequate for most users. However, extensive customization of a broad range of operational parameters is available to system administrators who wish to take advantage of the NetBlazer 40's rich capabilities. These facilities are described in the Advanced Configurations section of the *NetBlazer Configuration Guide*.

A complete listing of the NetBlazer 40's commands, along with comprehensive descriptions and examples of usage, is contained in the *NetBlazer Command Reference* manual.

FCC Warning

This equipment generates and uses radio frequency energy, and if not installed and used in strict accordance with the instructions in this manual, may cause interference to radio and television reception. It has been tested and found to comply with the limits for a Class A computing device under Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference in a commercial installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the system on and off, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna
- Relocate the system with respect to the receiver
- Move the system away from the receiver
- Plug the system into a different outlet so that the system and receiver are on different branch circuits.

If necessary, consult your dealer or any experienced radio/television technician for additional suggestions. You may find a booklet prepared by the FCC entitled *How to Identify and Resolve Radio-TV Interference Problems* helpful in resolving any problems. This booklet is available from the U.S. Government Printing Office, Washington DC 20402, Stock Number 004-000-00345-4.

Table of Contents

1. Introduction

Product Profile 1-1
Specifications 1-3
Electrical 1-3
Physical 1-3
Weight 1-3
Environmental 1-3
Options 1-3

2. Preinstallation Planning

General Planning 2-1
Ethernet Requirements 2-1
Token Ring Requirements 2-1
High-Speed Synchronous Interface Requirements 2-2
NS1 Single-Port Synchronous Board 2-2
SYN*xxx* Dual-Port Synchronous Board 2-3
Modem Requirements 2-4
ASYN8 Asynchronous Option 2-4
NM8 Asynchronous Option 2-4
Standard Asynchronous Ports (ASY00, ASY01, and Console) 2-4
Compatibility 2-5
Configuration Methods and Considerations 2-6
Using the NetBlazer Configuration Utility 2-6
Using the NetBlazer 40's Command Line Interface 2-6
Using DOS to Preconfigure the NetBlazer 2-7
Administrator's Workstation Requirements 2-7

3. NetBlazer 40 Options Installation

Option Board Factory Default Settings 3-1
Opening the NetBlazer 40 Case 3-2
Configuring and Installing Option Boards 3-2
Closing the NetBlazer 40 Case 3-3
Setting the AC Voltage Selector Switch 3-3
Connect the AC Power Cord 3-4
Administrator's Workstation 3-4
Setting Up a Dial-In Administrator's Workstation 3-4
Connecting a Terminal Directly to an Asynchronous Port 3-4

Appendix A, Checking the NetBlazer 40 Boot ROM Setup

Introduction 1

This manual provides instructions and related information required to install the NetBlazer 40. It is intended to be used by service personnel and qualified network administrators.

The Product Profile section of this chapter describes the applications for which the NetBlazer 40 is best suited. It also defines the elements on the NetBlazer 40's front and rear panels.

The Specifications section of this chapter provides basic electrical, physical, and environmental information. Also provided is a list of available options.

Product Profile

The NetBlazer 40 is the most powerful member of the NetBlazer family (see Figure 1-1). Featuring the fastest processor speed of the NetBlazer products and seven internal option slots, the NetBlazer 40 is well suited for the most demanding applications and can serve as many as 26 serial ports at speeds up to 115.2 Kbps.

The NetBlazer 40 is designed for large multiport applications that need a high-speed processor in applications where performance is critical. Applications for which the NetBlazer 40 is well suited include central sites that need 18 or 24 serial ports, leased-line and serial ports, or as a router for switched digital services such as ISDN and Switched 56.

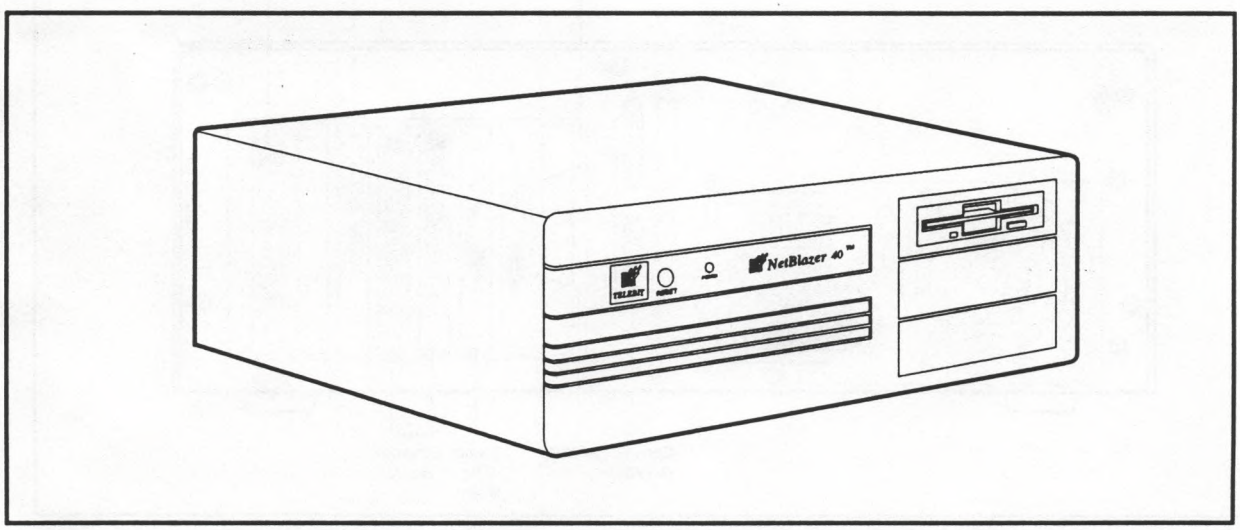


Figure 1-1. The NetBlazer 40

Figure 1-2 illustrates the NetBlazer 40 front panel. A RESET button is located on the left. To the immediate right of the reset button is the POWER LED, which is on when AC power is applied to the NetBlazer 40.

A standard 1.44-Mbyte 3.5-inch floppy diskette drive is located on the right.

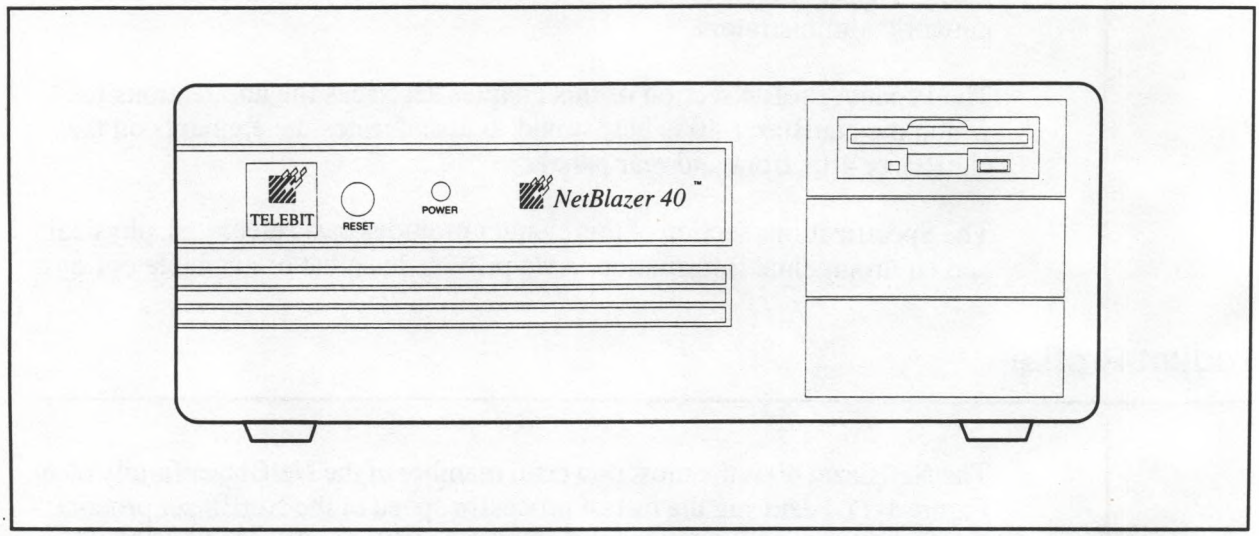


Figure 1-2. NetBlazer 40 Front View

Figure 1-3 illustrates the NetBlazer 40 rear panel with two Ethernet boards, one Token Ring board, one multiport asynchronous board, and one dual-port synchronous board installed.

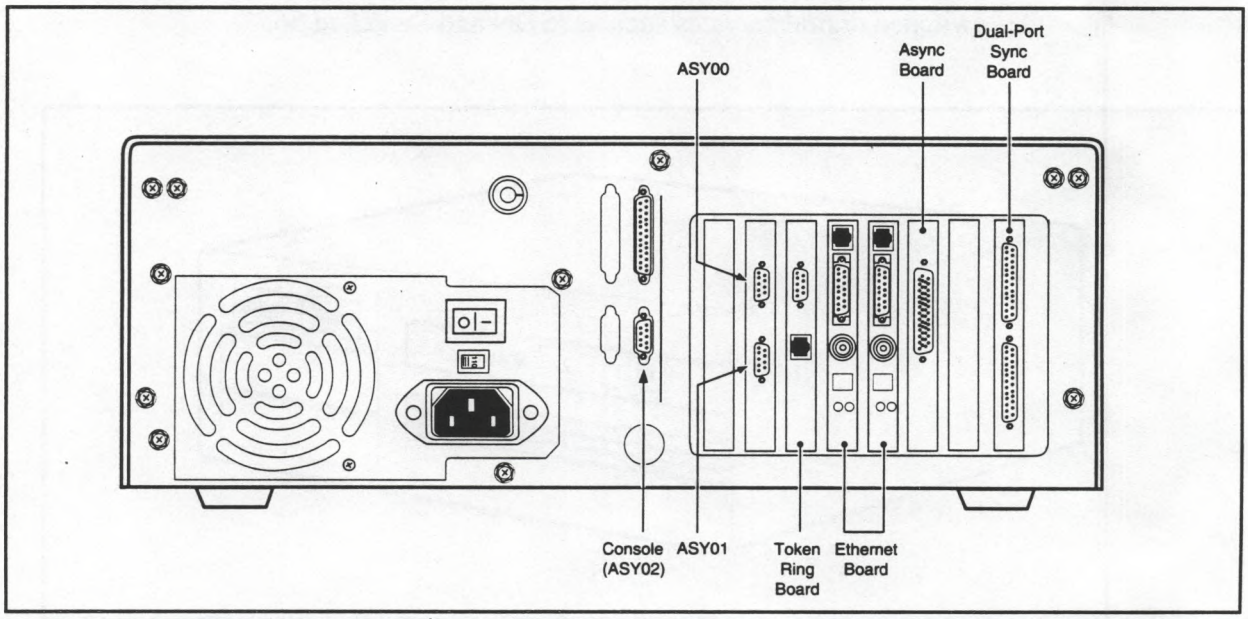


Figure 1-3. NetBlazer 40 Rear Panel

To the left of the option slots are the chassis I/O ports. The console port is an RS-232 serial port for use with an asynchronous terminal operating at 9600 baud (not recommended as a modem port). The parallel printer port is reserved for possible future use.

Note the two LED indicators on the Ethernet board. The red LED indicates network receive status (blinks while receiving data), while the green LED indicates twisted-pair network link status (off indicates a possible bad cable). The Ethernet ID number of the board is provided on an ID tag near the LEDs.

Specifications – NetBlazer 40

Electrical

120/220 VAC, 50/60 Hz, 200 watts

Physical

Dimensions: 16.7 inches wide x 16.7 inches deep x 6.18 inches high

Weight

Approximately 20 pounds without option boards

Environmental

Operating Temperature: 10–40° C

Humidity: 10–80% noncondensing

Options

Option Board Slots: Seven

Option Boards:

- NE1 Ethernet (up to three supported)
- NTR Token Ring (up to three supported)
- NM8 Multiport Asynchronous (one supported)
- ASYN8 Asynchronous (two supported)
- SYNxxx Dual-Port Synchronous (up to five supported)

Up to six option boards may be installed in the NetBlazer 40 (the standard I/O board always occupies one slot).

The Ethernet and Token Ring boards installed cannot total more than three of the same board or in combination.

Preinstallation Planning 2

This section overviews the cables, equipment, and prerequisite information needed to install and cable the NetBlazer 40. Before starting the installation, read this section to make sure that you have everything you need and to become familiar with what needs to be done to get the NetBlazer 40 ready to use as quickly as possible.

General Planning

Before installing the NetBlazer 40, decide where it will be located, and make sure that you have the appropriate number of AC outlets, telephone lines, and Ethernet or Token Ring connections and equipment needed to complete the installation. Avoid locating the unit in direct sunlight or near heating vents.

Ethernet Requirements

The NetBlazer 40 supports up to three Ethernet boards. Each Ethernet board can be connected to a local area network (LAN) using either the RJ-45 (10BaseT) connector, the BNC connector, or the 15-pin AUI connector. The BNC connector is used to connect to a thin Ethernet cable, whereas the AUI connector is used to connect the NetBlazer 40 to the Ethernet through an external transceiver.

You need to obtain any cables, hardware, and equipment required to connect the NetBlazer 40 to your network. Pinouts for the Ethernet board connectors are provided in Appendix A of the *NetBlazer Option Boards Installation Guide*.

Token Ring Requirements

The NetBlazer 40 supports up to three Token Ring boards. Each Token Ring board can be connected to a LAN using either the RJ-45 (UTP) connector or the 15-pin (STP) connector. The RJ-45 connector is used to connect to the ring with an unshielded twisted pair normally running at 4 Mbps, whereas the 15-pin shielded twisted-pair connector is used to connect rings running at 16 Mbps.

You need to obtain any cables, hardware, and equipment required to connect the NetBlazer 40 to your network. Pinouts for the Token Ring board connectors are provided in Appendix A of the *NetBlazer Option Boards Installation Guide*.

NS1 Single-Port Synchronous Board

If you have the NS1 single-port synchronous interface board installed in your NetBlazer 40, you need to obtain a data service unit/channel switching unit (DSU/CSU) or terminal adapter that supports a V.35, RS-422/RS-449, or an RS-232 interface.

The NS1 synchronous interface board is shipped from the factory configured for a DSU/CSU with a V.35 interface. Telebit provides the cable used to connect the NetBlazer 40 to a DSU/CSU using a V.35 interface. This cable configuration is shown in Figure 2-1.

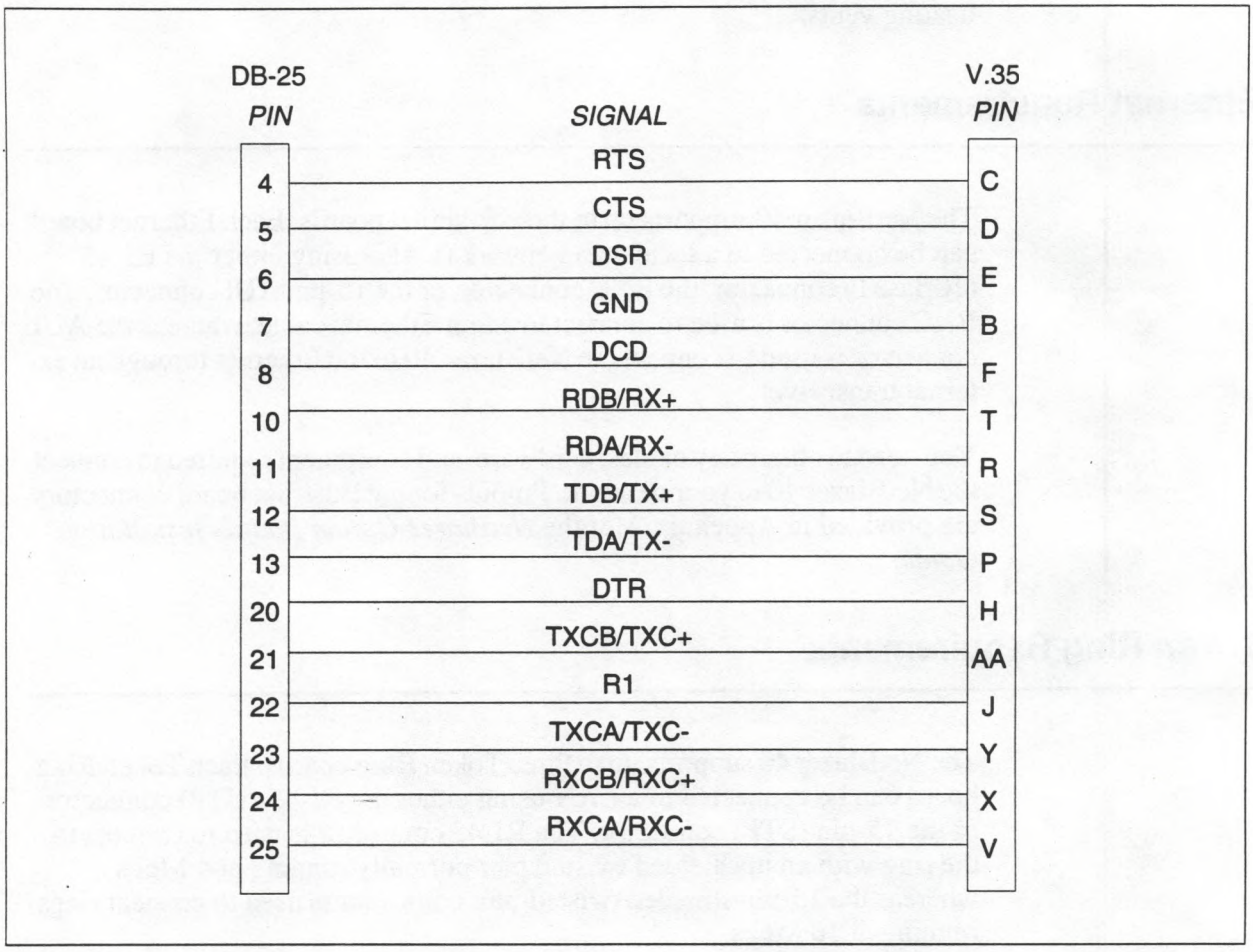


Figure 2-1. V.35 Cable Configuration

To connect the NetBlazer 40 to a DSU/CSU using an RS-422/RS-449 or an RS-232 interface, you need to reconfigure the synchronous interface board as described in the *NetBlazer Option Boards Installation Guide* and obtain an appropriate cable.

An RS-422/RS-449 interface requires a special cable with a male DB-25 connector for the NetBlazer 40 and a male DB-37 connector for the DSU/CSU. This cable should be configured as shown in Figure 2-2.

To use the RS-232 interface to the DSU/CSU, you need a straight-through RS-232 cable with a male DB-25 connector on each end of the cable.

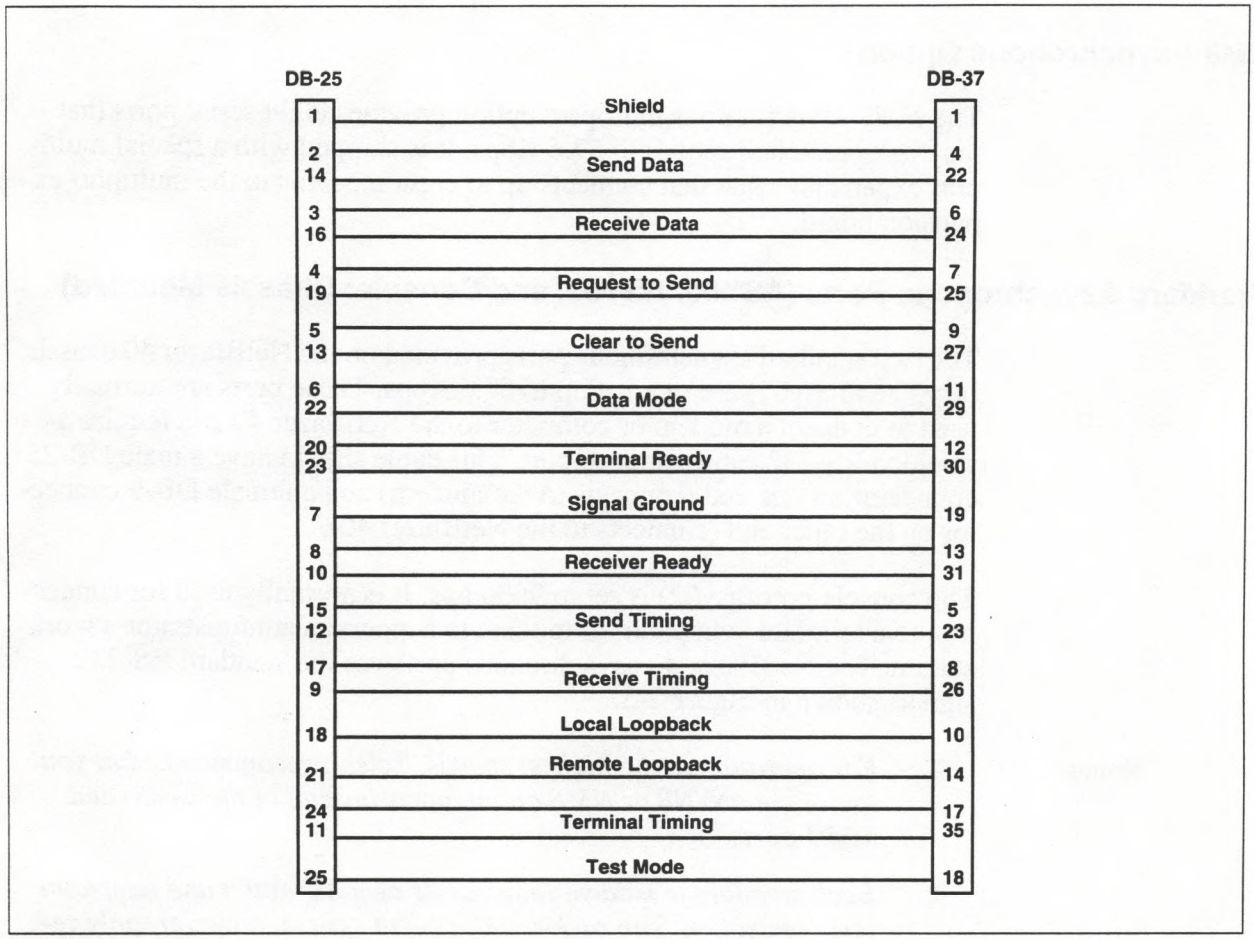


Figure 2-2. RS-422/449 Cable Configuration

SYN*xxx* Dual-Port Synchronous Board

If you have the SYN*xxx* dual-port synchronous interface board installed in your NetBlazer 40, you received the appropriate cables for the interface type specified when your initial order was placed. Note that if you want to use a T1/E1 line, you must attach this line to Port A. The B port can be used for connections up to 128 Kbps. Refer to the *NetBlazer Option Boards Installation Guide* for further information.

ASYN8 Asynchronous Option

Up to 26 standalone or rackmount modems can be connected to a NetBlazer 40 that contains two standard asynchronous ports, and one ASYN8 multiport asynchronous expansion board with three Modular Terminal Adapters (MTAs). (Additional MTAs are available from Telebit. Order model number ASYN8+.) The ASYN8 option is furnished with one MTA and the interconnecting cable, together which provide eight serial ports that may be operated to speeds of up to 115.2 Kbps.

NM8 Asynchronous Option

The NM8 asynchronous multiport option provides eight serial ports that may be operated at speeds to 57.6 Kbps. It is shipped with a special multiport expansion cable that connects up to eight modems to the multiport expansion board.

Standard Asynchronous Ports (ASY00, ASY01, and Console: Chassis Mounted)

The two standard asynchronous ports provided on the NetBlazer 40 chassis (asy00 and asy01) are rated at up to 57.6 Kbps. These ports are normally used to connect a modem or computer to the NetBlazer 40 and require a shielded RS-232 cable for each port. This cable should have a male DB-25 connector on one end (connects to the modem) and a female DB-9 connector on the other end (connects to the NetBlazer 40).

The console port (asy02) is set to 9600 bps. It is normally used for connection to a terminal, computer, or modem to support an administrator's workstation. The NetBlazer 40 asynchronous ports use the standard RS-232 signals shown in Figure 2-3.

Notes:

1. *For operation at the highest speeds, Telebit recommends that you use of the ASYN8 or NM8 option ports instead of the asy00 and asy01 ports.*

2. *Each standalone modem requires its own AC outlet and telephone line connection. The rackmount modem system, however, only requires one AC outlet and one RJ-23 telephone cable for each chassis.*

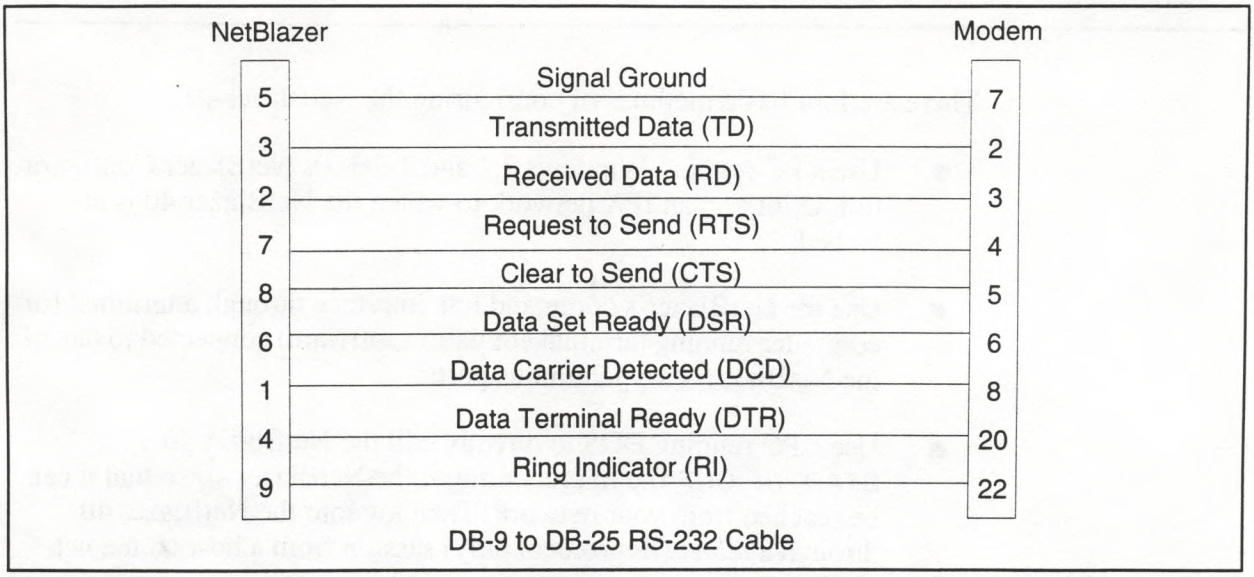


Figure 2-3. RS-232 Cable Configuration

Compatibility

The NetBlazer 40 currently supports the Telebit modems and firmware levels listed in Table 2-1. If you have a Telebit modem that is not at the required firmware level, contact your Telebit Technical Support representative for information about getting a firmware upgrade.

Table 2-1. Supported Telebit Modems

Modem	Firmware Level	Firmware Level for AppleTalk ARA Service
QBlazer	MA1.01 or later	
WorldBlazer SA or RM	LA5.00 or later	LA7.03 or later
T3000 SA or RM	LA5.00 or later	LA7.03 or later
T2500 SA or RM	GE6.01, GE7.00, GF7.00, or later	
T2000 SA or RM	BC5.00 or later	
T1600 SA	LA5.00 or later	LA7.03 or later
T1500 SA	GE6.01, GF7.00, or later	
T1000 SA	FA2.00 or later	
T1000 RM	FC2.00 or later	
TrailBlazer Plus SA or RM	BC7.00, GF7.00, or later	

There are four basic methods of configuring the NetBlazer 40:

- Use a PC running Windows 3.1 and Telebit's NetBlazer Configuration Utility on an IPX network to which the NetBlazer 40 is attached;
- Use the NetBlazer's command line interface through a terminal (or computer running terminal emulation software) connected to one of the NetBlazer's asynchronous ports;
- Use a PC running DOS to directly edit the NetBlazer 40's STARTUP.CNF file to preconfigure the NetBlazer 40 so that it can be reached from your network. Then log into the NetBlazer 40 through a *telnet* (IP protocol only) session from a host on the network;
- Use a Macintosh running a communications program that supports the Apple Communications Toolbox (i.e., MacTerminal 3.0 or PacerTerm), which is connected to the same network Ethernet segment as the NetBlazer 40. Use the NetBlazer's command line interface to perform the necessary configuration.

Using the NetBlazer Configuration Utility

Telebit recommends the use of its NetBlazer Configuration Utility. This utility provides a graphics-oriented user interface to the NetBlazer 40 for fast and easy configuration of the IP and IPX protocols over an IPX link.

Note: *The DOS PC used to run the NetBlazer Configuration Utility must be attached to the same Ethernet segment as the NetBlazer 40.*

Using the NetBlazer 40's Command Line Interface

If you are unable to use the NetBlazer Configuration Utility or prefer the use the NetBlazer's command line interface, you need an administrator's workstation (at least temporarily) to configure the NetBlazer 40 (see Figure 2-4). This can be done using one of two approaches:

- Connect a video display terminal or computer directly to the console port or to any unused asynchronous port (use an RS-232 null modem cable).
- Connect an on-site workstation to a modem and telephone line to dial into the NetBlazer 40 through the public switched telephone network (PSTN).

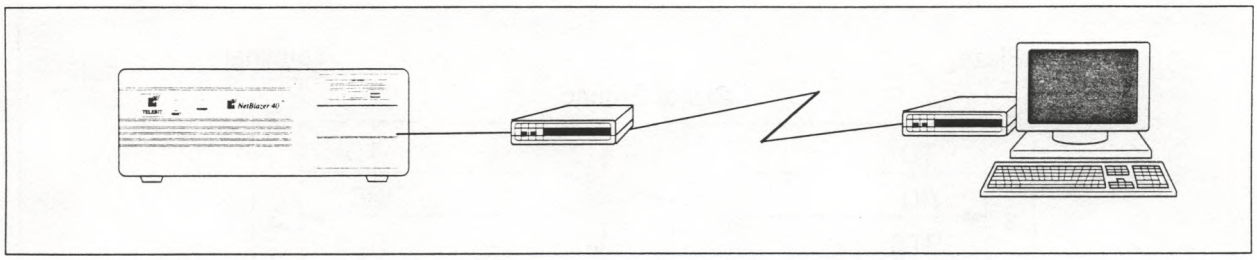


Figure 2-4. Dial-In Administrator's Workstation Configuration

Using DOS to Preconfigure the NetBlazer

To preconfigure the NetBlazer 40, edit the STARTUP.CNF file on the system diskette using a computer that supports 3.5-inch 1.44-Mbyte, DOS-formatted diskettes. Refer to the Getting Started section of the *NetBlazer Configuration Guide* for complete instructions.

Administrator's Workstation Requirements

To use a terminal (or computer running terminal emulation software) as an administrator's control terminal, you need an RS-232 null modem cable (Telebit part number 12724-01) or adapter. If you are constructing your own cable, refer to Figure 2-5. Your terminal (or computer) may require a different cable adaptation. However, when using a null modem cable or an adapter, observe the following requirements:

- The CTS signal to the NetBlazer 40 must be held active high (MARK).
- DSR and DCD must not be allowed to float.

  You may also need to connect an RS-232 gender changer to facilitate connecting an RS-232 cable between two DTE devices.

The second choice, dialing into the NetBlazer 40 from an on-site workstation, offers the advantage of testing the ability of the NetBlazer 40 to process incoming calls from a remote site. However, this method requires an additional modem and telephone line for the administrator's workstation.

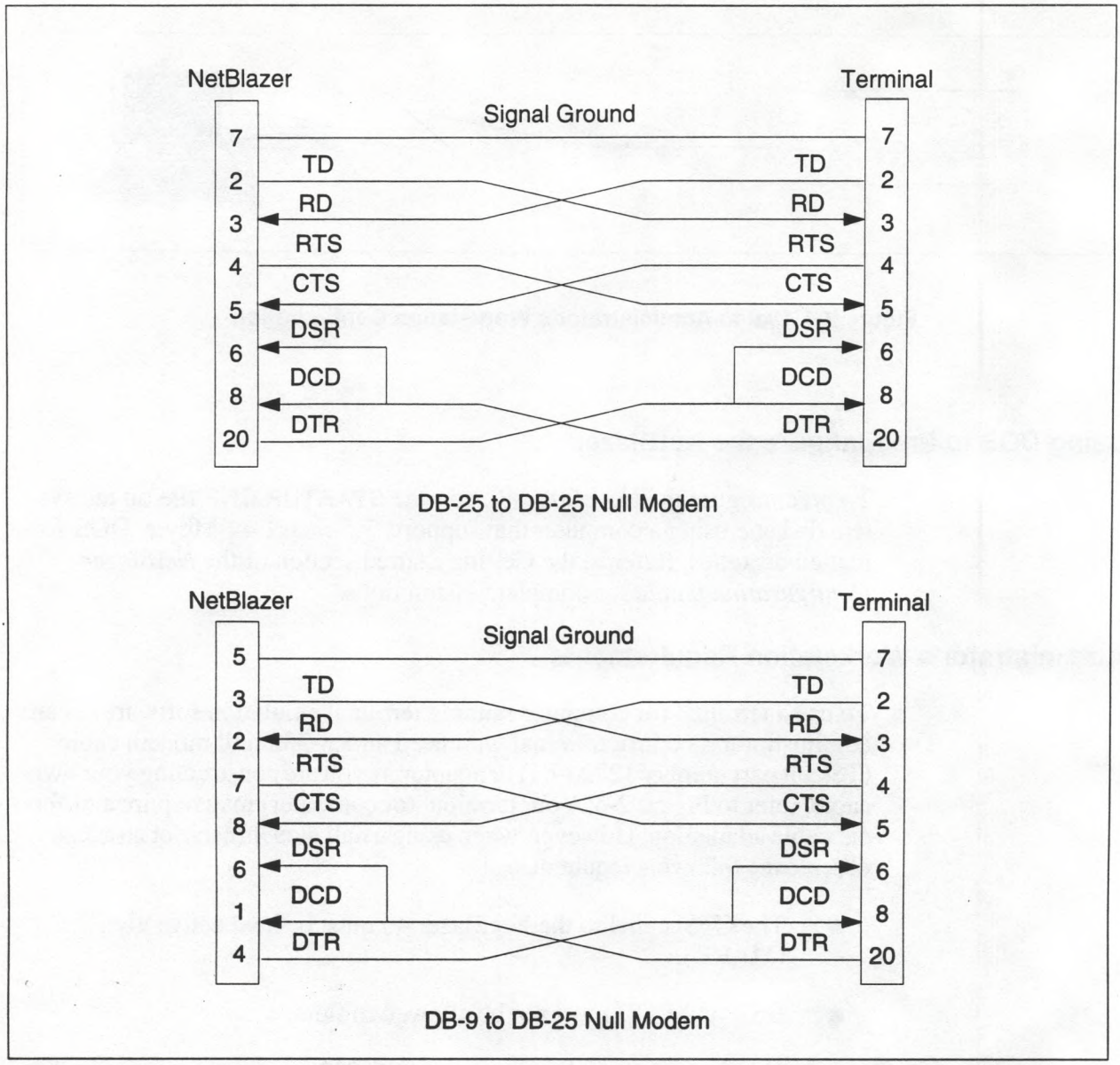


Figure 2-5. Null Modem RS-232 Cable Configurations

NetBlazer 40 Options Installation 3

This chapter provides instructions for installing the NetBlazer 40 and its associated optional hardware components.

Because the NetBlazer 40 is a high-end product that is normally tailored for specific applications, Telebit provides a single base model configurable to individual customer requirements.

Option Board Factory Default Settings

The NetBlazer option boards available for your NetBlazer 40 applications are shipped with factory default settings. If these defaults are correct for your installation, it is only necessary to install the option board in the NetBlazer 40 cabinet, as described in the *NetBlazer Option Boards Installation Guide*.

If your specific NetBlazer 40 operating environment involves a different option configuration (not the factory default settings) or LAN/DSU/CSU interface type other than identified above, additional hardware preconfiguration is necessary. Examples include:

- **Ethernet Media Type**. The Ethernet board is preset for connection to a thin (coax) Ethernet cable via the BNC connector. If you are connecting the NetBlazer 40 to an Ethernet network through an external transceiver, you must change jumpers on the Ethernet board to use the AUI connector. This is also true for the 10BaseT port.

- **Multiple Ethernet Boards**. Adding one or two Ethernet boards requires preconfiguring the IRQ level assigned to each board.

- **Token Ring**. Adding a Token Ring board (or boards) requires preconfiguring each board to the appropriate Token Ring speed and media type and setting the IRQ level assigned to each board.

- **Single-Port Synchronous Interface**. The high-speed synchronous interface board is shipped from the factory configured to connect to a DSU/CSU using a V.35 interface. If you are connecting the NetBlazer 40 to a DSU/CSU with an RS-422/449 or RS-232 interface, the four jumper plugs on the board must be repositioned for the appropriate interface.

- **Multiple Dual-Port Synchronous Interface Boards**. If you plan to install more than one SYN*xxx* board, you need to set switch SW2 on one of the boards to assign the board's base I/O address.

In all cases, the NetBlazer 40 case must be opened and the related hardware option must be preconfigured and installed for your particular requirements. Perform all of the following procedures that are applicable.

Opening the NetBlazer 40 Case

Warning: *Make sure that the NetBlazer ST is not connected to an AC power outlet; then open the NetBlazer ST case by performing the following steps:*

1. Using a Phillips screwdriver, remove the five screws on rear of the NetBlazer 40 top cover, as shown in Figure 3-1.

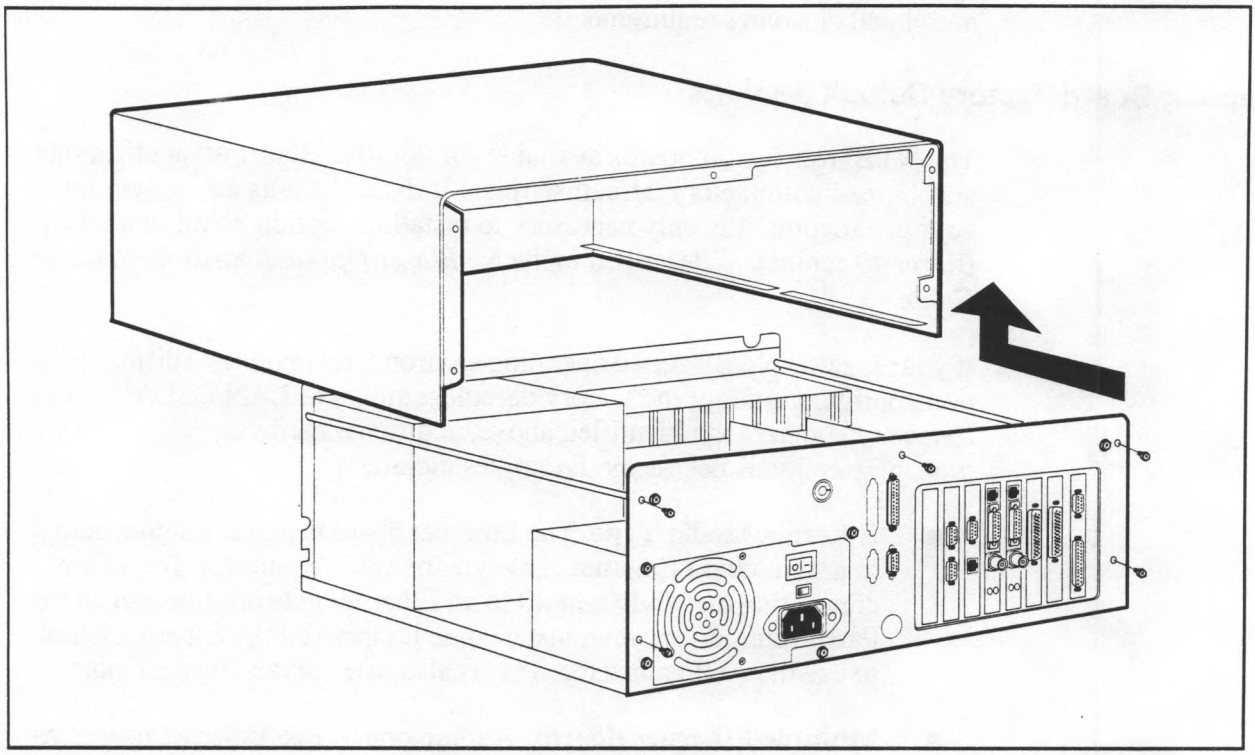


Figure 3-1. Removing the NetBlazer 40 Cover

2. Slide the top cover back about eight inches, then lift the top cover off the NetBlazer 40.

Configuring and Installing Option Boards

Refer to the *NetBlazer Option Boards Installation Guide* for details on configuring and installing option boards in the NetBlazer 40.

Caution: *The option boards are sensitive to static electricity. Observe ESD handling precautions and discharge any static on your body by touching an unpainted surface of the NetBlazer 40's frame before inserting the board*

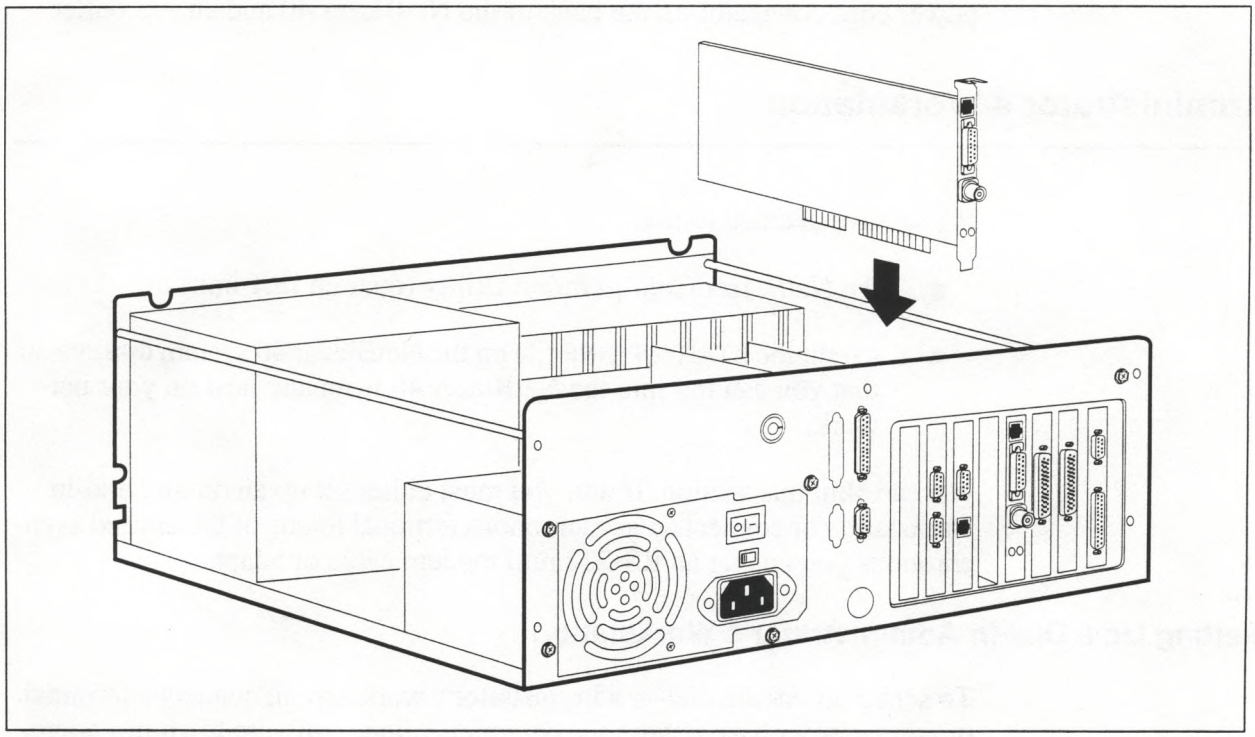


Figure 3-2. Board Insertion in to the NetBlazer 40

Closing the NetBlazer 40 Case

To close the NetBlazer 40 case, perform the following steps:

1. Lower the top cover onto the NetBlazer 40 so that the notches in the guide rails on the inside of the top cover align with the side edges of the front panel, and slide the top cover back into position.
2. Replace the five top cover mounting screws on the back of the system.

Setting the AC Voltage Selector Switch

Warning: *Before applying power to the NetBlazer 40, be certain that the voltage selector switch on the power supply rear panel is set to correspond with your line voltage (120 or 220 VAC)*

Connect the AC Power Cord

Connect the AC power cord supplied with your NetBlazer 40 between the power cord connector on the back of the NetBlazer 40 and an AC outlet.

Administrator's Workstation

If you have decided to use:

- the NetBlazer Configuration Utility (over an IPX link) or,
- to edit the STARTUP.CNF file on the NetBlazer 40 system diskette so that you can log into the NetBlazer 40 from any host on your network,

you can skip this section. If not, you must either set up an on-site dial-in workstation or connect an asynchronous terminal to one of the unused asynchronous ports using an RS-232 null modem cable or adapter.

Setting Up a Dial-In Administrator's Workstation

To set up an on-site dial-in administrator's workstation, connect a terminal or computer with asynchronous communications software to your modem, and connect the modem to the telephone network. Refer to the manual supplied with your modem for detailed instructions on how to install and configure the modem.

At the NetBlazer 40 site, connect the companion modem to:

- any one of the NM8 multiport octopus cable DB-25 connectors,
- any of the ASYN8 Modular Terminal Adapter (MTA) DB-25 connectors,
- the ASY00 or ASY01 9-pin connectors. Use a 9-pin to 25-pin modem cable when using the ASY ports.

Connecting a Terminal Directly to an Asynchronous Port

Choose which port to use as the control console port. The console port (asy02) is recommended, but ports asy00 or asy01 may also be used.

Note that the 25-pin printer port is reserved for possible future use.

Attach an RS-232 null modem cable or adapter between one of the ASY ports on the NetBlazer 40 and the RS-232 connector on your terminal or computer (see Figure 3-3). Wiring specifications for the null modem cable or adapter are discussed under the Administrator's Workstation Requirements section in Chapter 2 of this manual. You may also need to connect an RS-232 gender changer on the RS-232 cable to interconnect two DTE devices.

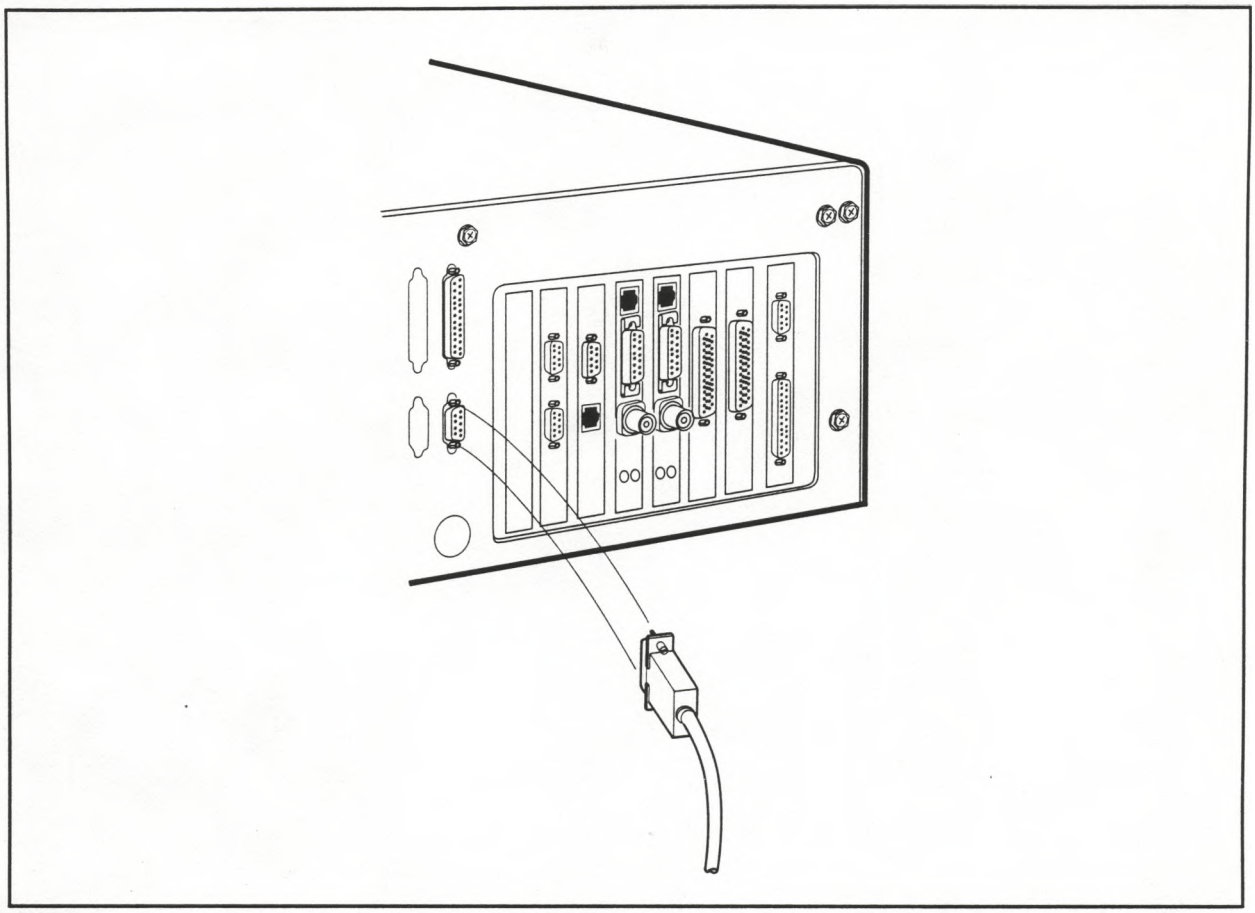
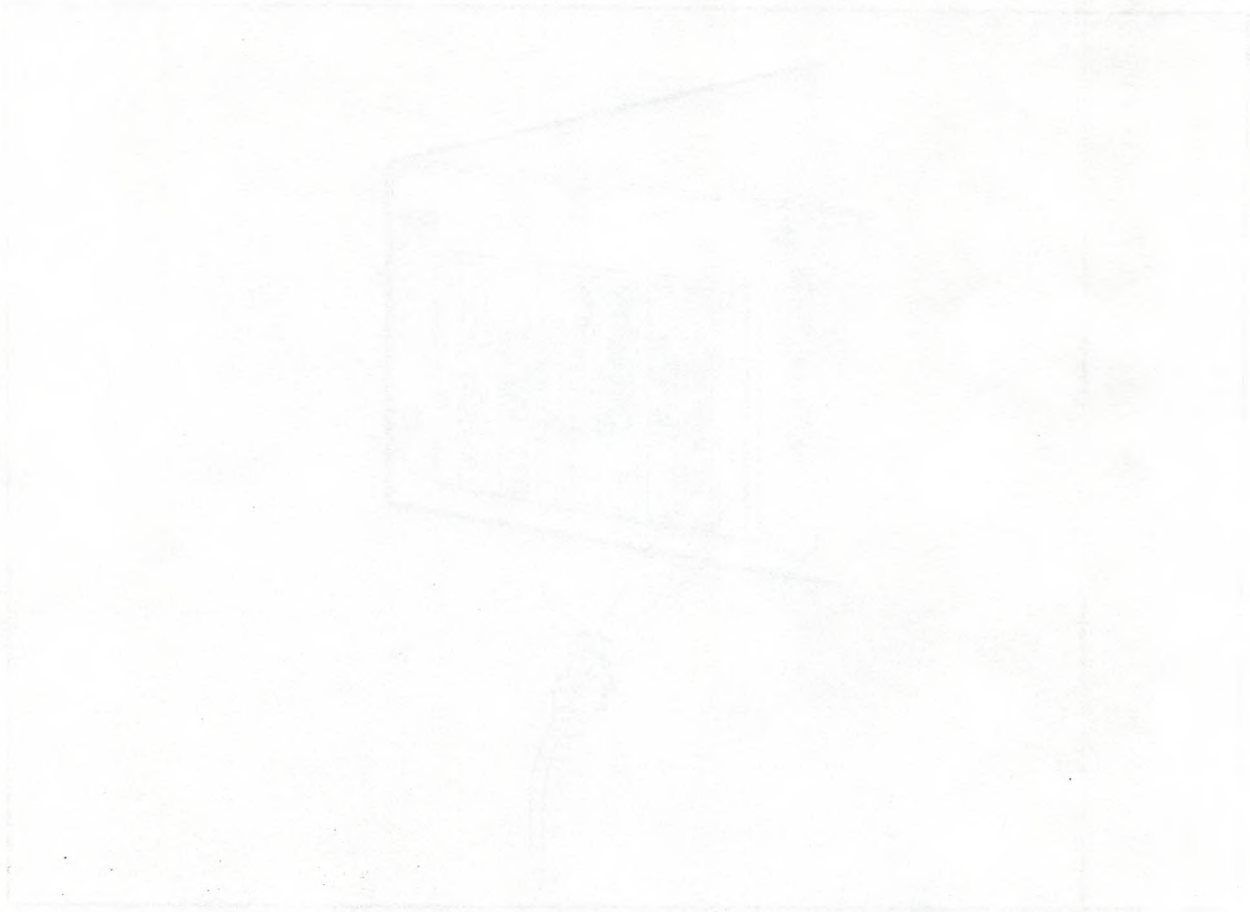


Figure 3-3. Dial-In Administrators Workstation Connections

Set your terminal to run at 9600 bps, 8 data bits, no parity, and 1 stop bit.



Checking the NetBlazer 40 Boot ROM Setup

A

If the NetBlazer 40 will not boot, there may be a problem with the boot ROM. Make sure that you have an asynchronous terminal (or computer running a terminal emulation program set to 9600 bps, 8 data bits, one stop bit, and no parity) connected (through a null modem cable) to the console port on the back of the NetBlazer 40. Perform the following steps to check the ROM settings:

1. Remove the NetBlazer 40 system diskette, then turn on the NetBlazer 40. The following information should be displayed on your terminal screen.

```
640K  Base Memory
4096K Total Memory
64K Cache Installed

TELEBIT ROM version 2.00
Copyright (c) 1985-1992 Landmark Research Int'l Corp.
All rights reserved.

Press "B" for boot or "S" for setup
```

2. Press the **s** key to view the current ROM settings.

```
T E L E B I T   S E T U P
Version 2.00
Copyright (c) 1985-1992 Landmark Research Int'l Corp.
ALL RIGHTS RESERVED

Current date: 1/21/92
Current time: 11:07:15
Diskette A: 1.44 Megabyte drive (3.5")
Diskette B: Not Installed
Hard Disk 0: Not Installed
Hard Disk 1: Not Installed
Base Memory: 640 KiloBytes
Extended Memory: 3,456 KiloBytes
Cache limited to 4 Megabytes
Primary display: Monochrome display (MDA)

("Yes" or <ENTER> will reboot system
Is this correct ("Yes", <ENTER>, "No", or <ESC>?
```

3. The drive and memory configuration settings displayed on your screen should match the settings shown above.

   If the settings displayed on your screen are correct, enter **y** . Insert your working copy of the NetBlazer 40 system diskette and press the Enter or Return key to reboot the NetBlazer 40. If the system still will not boot, contact your technical support representative.

If the settings displayed are not correct, enter **n** to begin the setup dialog, which allows you to make changes to the current setup options.

```
Current Date: 02/21/1992
Current Time: 13:26:35

Is this correct ("Yes", <ENTER>, "No", or <ESC>?
```

4. If the current date and time displayed are correct, press the Enter or Return key to continue. Otherwise, enter **no** and press the Enter or Return key. Enter today's date in the format shown (be sure to use four numeric characters for the year).

```
Current time: 14:46:36

Type new time (HH:MM:SS) or <ENTER> to accept?
```

5. If the current time displayed is correct, press the Enter or Return key to continue. Otherwise, enter the time in the format shown. Note that the NetBlazer uses a 24-hour clock; e.g., 1:00 p.m. is entered as 13:00:00, and 11:59 p.m. is entered as 23:59:00.

```
Current date: 02/21/1992
Current time: 15:01:50

Is this correct ("Yes", <ENTER>, "No", or <ESC>)? yes
```

6. Verify that the current date and time is correct by entering **yes** to the above prompt.

```
Base Memory: 640 Kilobytes


Is this correct ("Yes", <ENTER>, "No", or <ESC>)?
```

7. The NetBlazer 40 is shipped with the maximum amount of base memory of 640 Kbytes. If the base memory displayed is not equal to 640 Kbytes, answer **no** to the above prompt and enter **640** when prompted for the base RAM size in kilobytes. Normally this should not need to be changed.

```
Extended Memory: 1,408 Kilobytes
Cache limited to 4 Megabytes

Is this correct ("Yes", <ENTER>, "No", or <ESC>)?
```

8. The NetBlazer 40 is shipped with 3,456 Kbytes of extended memory. If the extended memory displayed is not equal to 3,456 Kbytes, answer **no** to the above prompt and enter **3,456** when prompted for the extended RAM size in kilobytes.

```
Limit caching to 4 Megabytes?
Is this correct ("Yes", <ENTER>, "No", or <ESC>)?
```

9. The NetBlazer 40 uses cache memory. Enter **yes** to the above prompt to proceed.

```
Primary display: Monochrome display (MDA)

Is this correct ("Yes", <ENTER>, "No", or <ESC>)?yes
```

10. Because the NetBlazer 40 currently does not come with an internal video display board, this setting is insignificant. Enter **yes** to the above prompt to proceed.

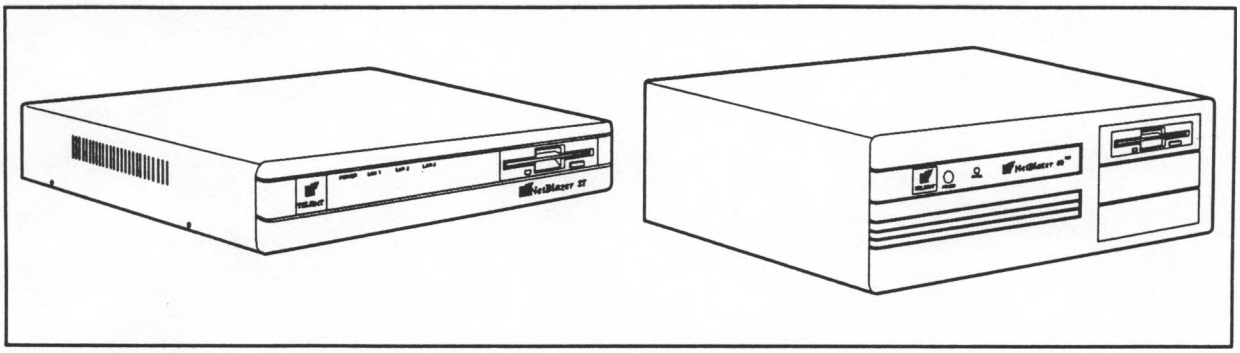
```
Diskette A: 1.44 Megabyte drive (3.5")
Diskette B: Not Installed

Is this correct ("Yes", <ENTER>, "No", or <ESC>)?yes
```

11. The NetBlazer 40 is shipped with one 3.5-inch 1.44-Mbyte diskette. If the diskette information displayed is incorrect, answer **no** to the above prompt. Enter **4** to select a 1.44-Mbyte drive when prompted for the type for drive A, and enter **0** to select drive B.

```
Hard Disk 0: Not Installed
Hard Disk 1: Not Installed

Is this correct ("Yes", <ENTER>, "No", or <ESC>)?yes
```

12. The NetBlazer 40 system currently does not support a hard disk drive. If the internal hard disk information displayed is incorrect, answer **no** to the above prompt. Enter **0** when prompted for the number of hard disk drives.

```
T E L E B I T   S E T U P
Version 2.00
Copyright (c) 1985-1992 Landmark Research Int'l Corp.
ALL RIGHTS RESERVED

Current date: 02/21/1992
Current time: 15:16:30
Diskette A: 1.44 Megabyte drive (3.5")
Diskette B: Not Installed
Hard Disk 0: Not Installed
Hard Disk 1: Not Installed
Base Memory: 640 Kilobytes
Extended Memory: 3,456 Kilobytes
Cache limited to 4 Megabytes
Primary display: Monochrome display (MDA)

("Yes" or <ENTER> will reboot system)
Is this correct ("Yes", <ENTER>, "No", or <ESC>)? yes
```



NetBlazer Option Boards

Installation Guide

NetBlazer Option Boards

90269-01

How to Use This Manual

This manual is a guide to installing the NetBlazer option boards. It is intended as a companion to the NetBlazer Installation Guides.

This manual covers consists of four chapters:

- Chapter 1, NE1 Ethernet Board Installation, provides an overview of the NE1 Ethernet board, configuring the board, and connecting it to your Ethernet local area network (LAN).
- Chapter 2, NTR (Token Ring) Board Installation, provides an overview of the NTR Token Ring board, configuring the board, and connecting it to your Token Ring LAN.
- Chapter 3, Synchronous Board Installation, covers two models of synchronous boards, the NS1 single-port board and the SYN*xxx* dual-port board. The section provides an overview of each board, its configuration, and connecting it to a CSU/DSU or ISDN terminal adapter.
- Chapter 4, Asynchronous Board Installation, covers two models of asynchronous boards: the NE1 multiport board and the ASYN8 and its multiple terminal adapter (MTA) modules. The section provides an overview of each board, its configuration, and connecting it to asynchronous devices.

Three appendixes are provided. Appendix A, Interface Board Pinouts, provides detailed connector pinouts of each option board. Appendix B, MTA Line Assignment Record, includes a convenient fill-in-the-blank worksheet to provide a record of your asynchronous line assignments when using the ASYN8 board. Appendix C, Other Ethernet Board Configurations, provides configuration information on earlier generation NetBlazer Ethernet boards.

Related Documentation

Refer to your NetBlazer Installation Guide for details about removing the NetBlazer's cover and installing the option boards.

Table of Contents

How to Use This Manual ..... **i**

Related Documentation i

NE1 Ethernet Board Installation **1-1**

Factory Default Option Settings 1-1
Open the NetBlazer Case 1-1
Configuring the Ethernet Board 1-2
- Thin Ethernet (10Base2) Setup 1-2
- Thick Ethernet (10Base5) Setup 1-2
- RJ-45 Setup (10BaseT) 1-3
- Installing or Replacing the Ethernet Board 1-4

Closing the NetBlazer Case 1-4
Connecting the Ethernet Board to the LAN 1-4
- Connecting to a Thin Ethernet (10Base2) Network 1-4
- Connecting to a Thick Ethernet (10Base5) Drop 1-5
- Connecting to an RJ-45 Twisted Pair (10BaseT) 1-6

NTR (Token Ring) Board Installation **2-1**

Factory Default Option Settings 2-1
Opening the NetBlazer Case 2-1
Configuring the Token Ring Board 2-1
- Ring Speed 2-1
- Media Selection 2-2
- IRQ and Base I/O Address 2-2
- Install the Token Ring Board 2-3

Closing the NetBlazer Case 2-3
Connecting the Token Ring Board to the Ring 2-3
- UTP (RJ-45) Connection 2-3
- STP (DB-9) Connection 2-4

Synchronous Board Installation **3-1**

Factory Default Settings 3-1
Opening the NetBlazer Case 3-1
Configuring the Single-Port Synchronous Board (NS1) 3-2
- V.35 3-2
- RS-232 or RS-422/RS-449 3-2

Configuring the Dual-Port Synchronous Board (SYN*xxx*) 3-5
- Setting Switches on the Dual-Port Synchronous Board 3-6

Closing the NetBlazer Case 3-7
Connecting the Synchronous Board to a DSU/CSU 3-7
Connecting the Synchronous Board to an ISDN TA 3-8

Asynchronous Board Installation **4-1**
NM8 Multiport Board 4-1
External Modems 4-2
ASYN8 Multiport Asynchronous Board 4-3
Factory Default Option Settings 4-3
Opening the NetBlazer Case 4-3
Installing the ASYN8 Asynchronous Board 4-4
Closing the NetBlazer Case 4-4
Configuring the MTAs 4-4
Connecting the ASYN8 Board to the MTA 4-7
Connecting to the ASYN8 MTA RS-232 Ports 4-7
MTA Rackmount Adapter 4-8
Line Designations 4-8

Interface Board Pinouts **A-1**

MTA Line Assignment Record **B-1**

Other Ethernet Board Configurations **C-1**

NE1 Ethernet Board Installation 1

This chapter provides instructions for installing the model NE1 Ethernet board in a NetBlazer. This board supersedes the previous EN1 board (see Appendix C) and provides an RJ-45 twisted-pair port (for 10BaseT) in addition to the thin Ethernet (BNC connector) and the AUI port.

Note: *If you plan to boot the NetBlazer remotely from a bootp server, the NetBlazer's en0 interface must be on the same Ethernet segment as the bootp server or on the same Ethernet segment as another NetBlazer with the bootp forwarding function enabled. In the latter case, the second NetBlazer is used to forward bootp requests to the network bootp server. Refer to the Network Management section of the* NetBlazer Configuration Guide *for details.*

Factory Default Option Settings

As shipped from the factory, the NE1 Ethernet board is preset to the following configuration:

- **10Base2 Media Type**. The Ethernet board is preset for connection to a thin (coax) Ethernet cable via the BNC connector. If you are connecting the board to an Ethernet network through an external transceiver, you must change jumpers on the Ethernet board to use the AUI connector. This is also true for the 10BaseT port.
- **IRQ 3, I/O Base Address 280h**. These will need to be reset according to your system requirements.

If your specific Ethernet requirements involve a different configuration (not the factory default settings) than identified above, jumper changes on the board are necessary.

Perform the following procedures that are applicable.

Open the NetBlazer Case

Warning: *Make sure that the NetBlazer is not connected to an AC power outlet; then open the NetBlazer case by performing the following steps:*

1. Using a Phillips screwdriver, remove the screws on rear or sides of the NetBlazer top cover, as shown in Figure 3-1 of your *NetBlazer ST or 40 Installation Guide*.
2. Slide the top cover back and lift the top cover off the NetBlazer.

Thin Ethernet (10Base2) Setup

This is the factory default setting (BNC connector). No further configuration is necessary unless you are adding an additional board(s). In this case, skip to the IRQ and Base I/O Address section.

Thick Ethernet (10Base5) Setup

If you are connecting a thick Ethernet using an external transceiver on the AUI connector on the Ethernet board, perform the following steps:

Caution: *The Ethernet board is sensitive to static electricity. Observe ESD handling precautions and discharge any static on your body by touching an unpainted surface of the NetBlazer's frame before inserting the board.*

1. Remove the mounting screw on the Ethernet board and rock the board out of its socket. (If installing a new board, skip this step.)
2. Locate jumpers JP8 and JP11 (see Figure 1-1). The jumper plug on JP8 should be on the bottom two pins.

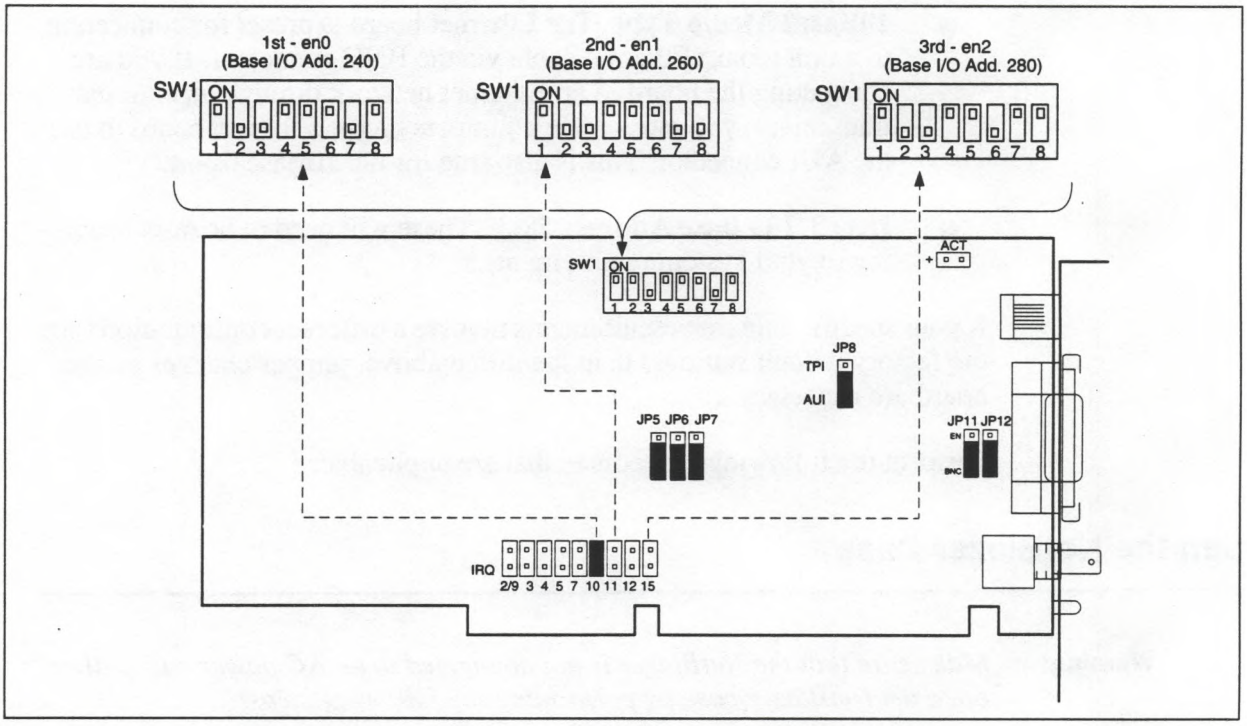


Figure 1-1. Ethernet Board Jumpers (AUI, en0)

3. JP11 is the BNC enable jumper. Place the jumper plug on JP11 on the bottom two pins (BNC disabled).

RJ-45 Setup (10BaseT)

To configure the Ethernet board to use the RJ-45 port, first remove the board as described above (if applicable). Then perform the following steps:

1. Move the jumper plug on JP11 on the bottom two pins (BNC disabled).
2. Move the jumper plug on JP8 to connect the top two pins.

Table 1-1 summarizes the media type selection jumpers.

Table 1-1. Ethernet Media Selection Jumpers

Media Type	JP8	JP11
Thin (BNC) *Default*		
Thick (AUI) (10Base5)		
RJ-45 (10BaseT)		

IRQ and Base I/O Address

Both the Ethernet and Token Ring boards share the same set of interrupts. When configuring a NetBlazer containing multiple Ethernet boards or mixed Ethernet and Token Ring boards, it is very important that the appropriate IRQs and base I/O addresses be set correctly.

The IRQ jumper bank on the lower edge of the board assigns the IRQ level, while switch SW1 assigns the corresponding base I/O address. Refer to Figure 1-1 and Table 1-2 for the setting appropriate for your installation.

Table 1-2. Ethernet IRQ Level and Base I/O Address Assignments

Ethernet Board	IRQ	Base Address (SW1)
en0	10	240h
en1	11	260h
en2	15	280h

Installing or Replacing the Ethernet Board

After completing all preconfiguration changes, install (or reinstall) the Ethernet board. Carefully guide the board into its slot (as shown in your *NetBlazer ST or 40 Installation Guide*) so that the board's edge connector is aligned with the slot connector and the AUI/BNC connectors extend through the slot opening. Then, firmly press on the top edge of the board until it is securely mated with its connector, and replace the Ethernet board mounting screw.

ST Installation

If you are installing (or reinstalling) the Ethernet board in a NetBlazer ST, reconnect the activity LED cable to the connector (ACT) on the board edge: orange/black = LAN1, red/black = LAN2, yellow/black = LAN3. Note that black is negative and the color is positive.

Closing the NetBlazer Case

Close the NetBlazer case (see Chapter 3 of your *NetBlazer ST or 40 Installation Guide*). Connect the AC power cord supplied with your NetBlazer between the power cord connector on the back of the NetBlazer and an AC outlet.

Connecting the Ethernet Board to the LAN

Connecting to a Thin Ethernet (10Base2) Network

Perform the following steps to connect the Ethernet board to a thin Ethernet cable using a T connector, as illustrated in Figure 1-2.

1. Attach the thin Ethernet cable to both ends of a T connector. If the NetBlazer is the last device on the cable, attach a 50-ohm terminator to one end of the connector. Neither side of the T connector should be left open.
2. Plug the T connector into the BNC connector on the Ethernet board. Turn the T connector sleeve clockwise to lock in place.

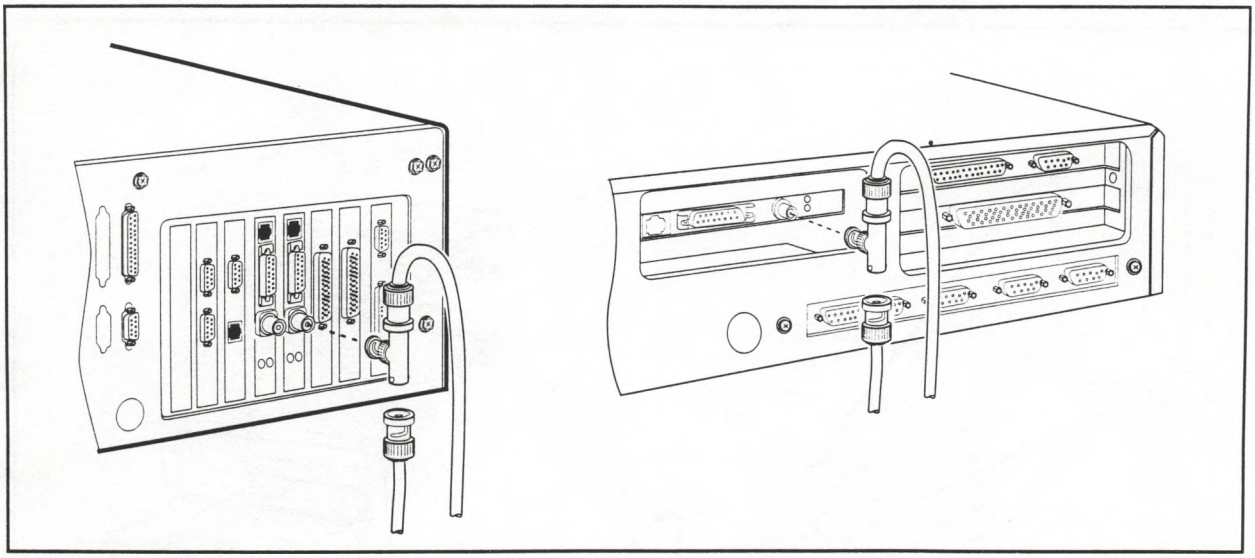


Figure 1-2. Thin Ethernet Connection

Note: *The illustrations used throughout this guide show the Ethernet board in both horizontal (NetBlazer ST) position and vertical (NetBlazer 40) position.*

Connecting to a Thick Ethernet (10Base5) Drop

Before connecting the NetBlazer to a thick Ethernet line, jumpers JP8 and JP11 on the Ethernet board must be set to use the AUI connector.

Connect an AUI dropcable between the NetBlazer's Ethernet board and an external transceiver by performing the following steps:

1. Follow the instructions provided with your external transceiver to attach the transceiver to the network and attach the female end of the AUI dropcable to the transceiver.
2. Plug the male end of the dropcable into the AUI connector shown in Figure 1-3.
3. Push the sliding latch mechanism on the AUI connector down to secure the connector. The sliding latch is snug and may require some effort to lock in place.

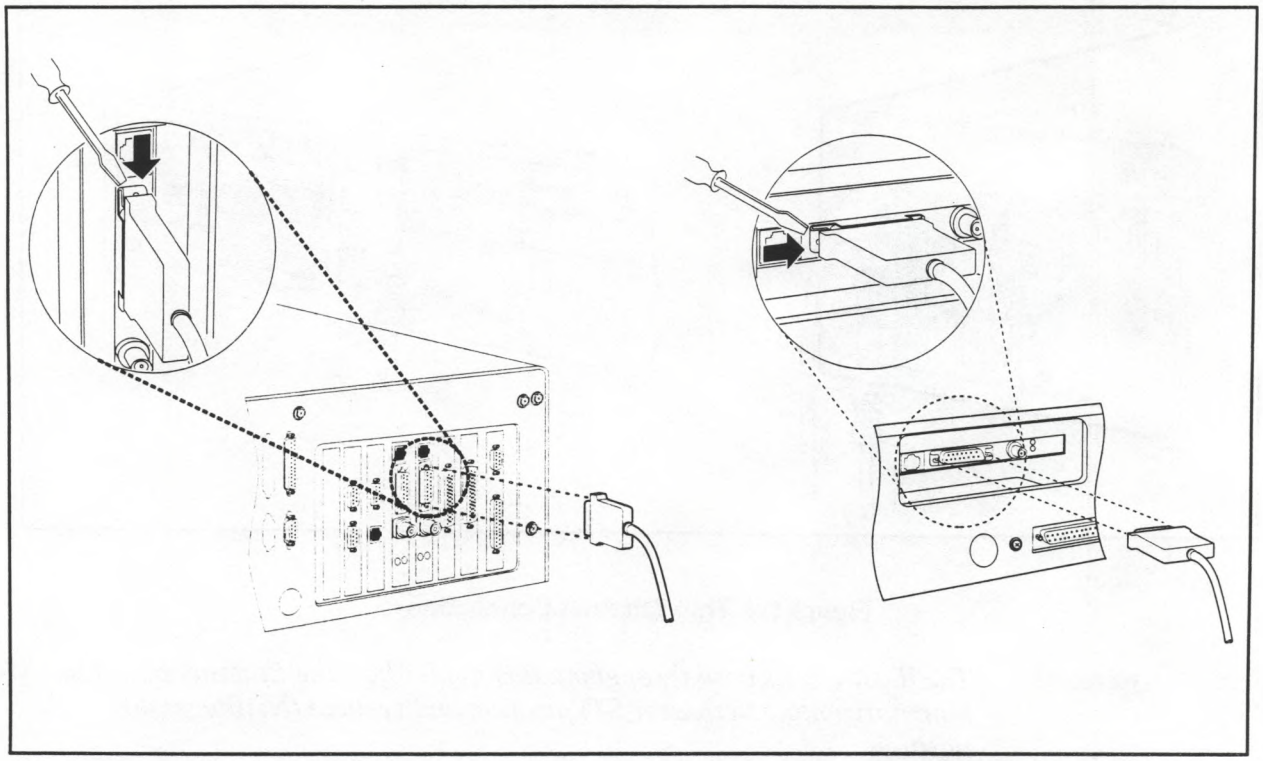


Figure 1-3. Ethernet AUI Connection

Connecting to an RJ-45 Twisted Pair (10BaseT)

Before connecting the Ethernet board to a twisted-pair drop, you must first have jumpers JP8 and JP11 on the Ethernet board set to use the RJ-45 connector.

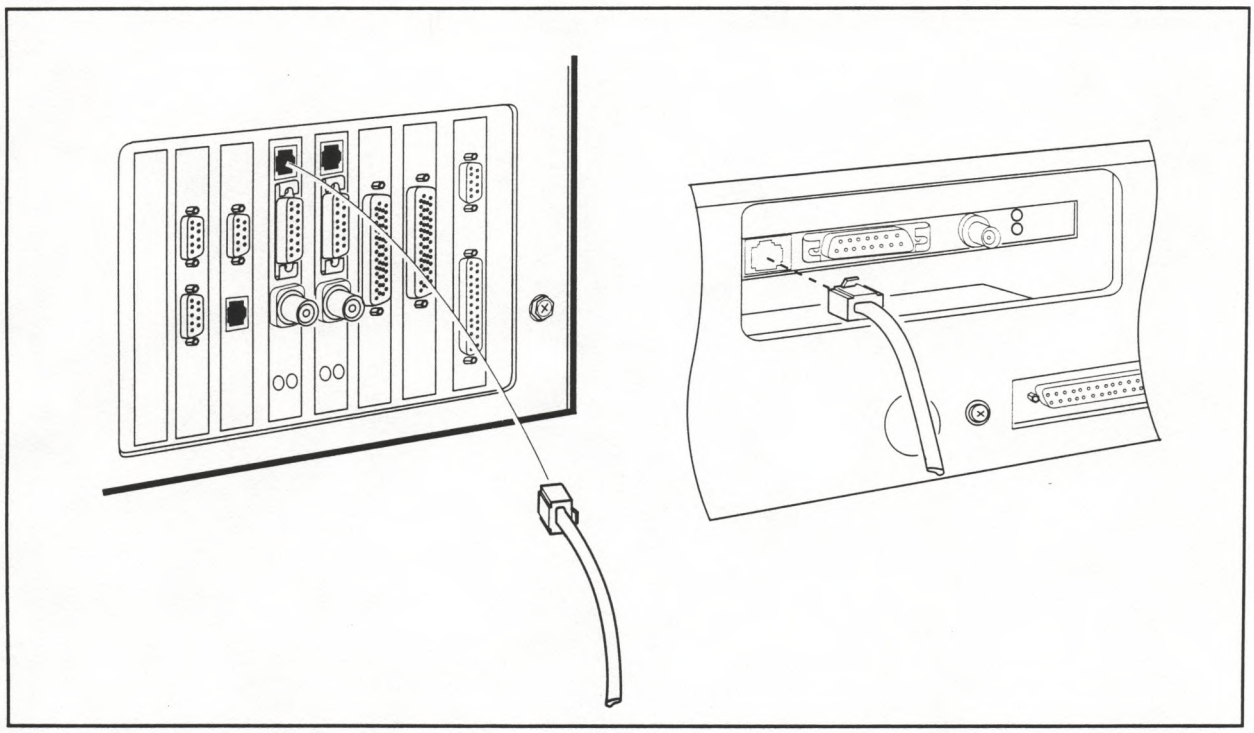


Figure 1-4. Ethernet RJ-45 Connection

Plug the RJ-45 cable connector into the female RJ-45 on the Ethernet board, as shown in Figure 1-4.

NTR (Token Ring) Board Installation 2

This chapter provides instructions for installing the NTR Token Ring board in a NetBlazer.

Factory Default Option Settings

As shipped from the factory, the Token Ring board is set to use the RJ-45 port for use with an unshielded twisted pair (SW4) operating at a network speed of 4 Mbps (SW2), while the IRQ is assigned to level 12 (SW1). If these setting are not appropriate to your application, make the necessary changes as described in Figure 2-1 and Table 2-1.

If your specific Token Ring requirements involve a different configuration (not the factory default settings) than identified above, jumper changes on the board are necessary.

Perform the following procedures that are applicable.

Opening the NetBlazer Case

Warning: *Make sure that the NetBlazer is not connected to an AC power outlet; then open the NetBlazer case by performing the following steps:*

1. Using a Phillips screwdriver, remove the screws on rear or side of the NetBlazer top cover as shown in Figure 3-1 of your *NetBlazer ST or 40 Installation Guide.*
2. Slide the top cover back and lift it off the NetBlazer.

Configuring the Token Ring Board

Caution: *The Token Ring board is sensitive to static electricity. Observe ESD handling precautions and discharge any static on your body by touching the NetBlazer's frame before inserting the board.*

Ring Speed

Switch SW2-8 must be set to match the speed at which your Token Ring is operating. Up selects 4 Mbps; down selects 16 Mbps (see Figure 2-1).

Media Selection

The Token Ring board supports both shielded twisted-pair (STP) media and unshielded twisted-pair (UTP) media through switch SW4. Position 2 (on the right) selects UTP, and position 1 (on the left) selects STP.

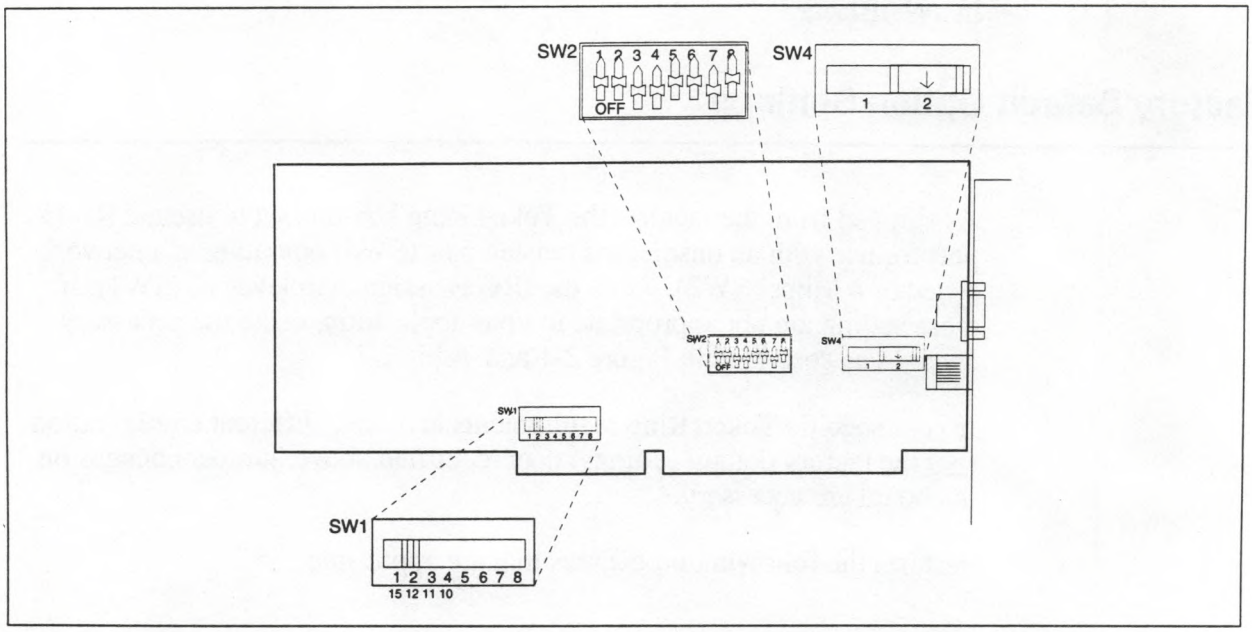


Figure 2-1. Token Ring Board Switch Settings

IRQ and Base I/O Address

Both the Token Ring and Ethernet boards share the same set of interrupts. When configuring a NetBlazer containing multiple Token Ring boards, Ethernet boards, or mixed Ethernet and Token Ring boards, it is very important that the appropriate IRQs and base I/O addresses be set correctly.

Switch SW1 assigns the IRQ level, while SW2 sets the corresponding base I/O address. See Table 2-1 for the setting appropriate to your configuration.

Table 2-2. Token Ring IRQ Level and Base Address Assignments

Token Ring Board	IRQ (SW1)	Base Address (SW2)
tr0	12	0A20
tr1	15	1A20
tr2	11	2A20

Note: *Switch SW3 (DMA Channel) setting is ignored by the NetBlazer software. Factory default settings are silkscreened on the solder side of the board.*

Install the Token Ring Board

After completing all preconfiguration changes, install the Token Ring board. Carefully guide the board into its slot so that the board's edge connector is aligned with the slot connector and the cable connectors extend through the slot opening. Then, firmly press on the top edge of the board until it is securely mated with its connector, and install the Token Ring board mounting screw.

Closing the NetBlazer Case

Close the NetBlazer case as described in Chapter 3 of your *NetBlazer ST or 40 Installation Guide*.

Connect the AC power cord supplied with your NetBlazer between the power cord connector on the back of the NetBlazer and an AC outlet.

Connecting the Token Ring Board to the Ring

UTP (RJ-45) Connection

To connect the NetBlazer to an unshielded twisted pair (UTP) network, attach the UTP RJ-45 cable to the female RJ-45 connector on the Token Ring board, as illustrated in Figure 2-3.

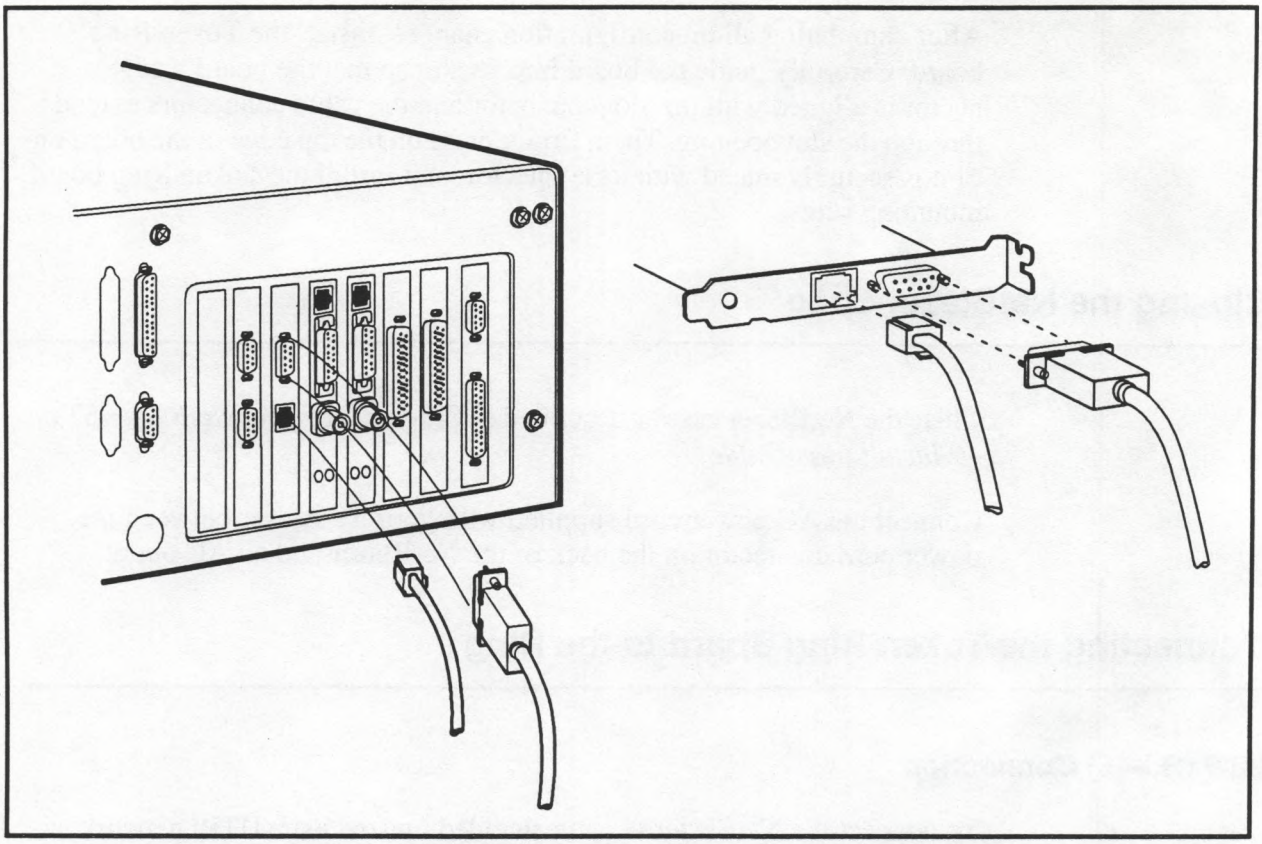


Figure 2-3. Token Ring Connections

STP (DB-9) Connection

Before connecting the Token Ring board to an STP, the cabling media switch SW4 on the Token Ring board must be set to use the STP connector (DB-9) as described in the Configuring the Token Ring Board section in this chapter.

Connect the STP dropcable to the NetBlazer's Token Ring board by plugging the male end of the cable into the 9-pin D connector, as shown in Figure 2-3. Tighten the retaining screws to prevent the cable from being pulled loose.

Synchronous Board Installation 3

This document provides instructions for installing both the Telebit single-port and dual-port synchronous interface boards in a NetBlazer chassis. This procedure involves two basic operations: setting the base I/O address and configuring the board for the desired interface.

Factory Default Settings

As shipped from the factory, a synchronous board is preset to the following configuration:

- **NS-1 single-port board:** I/O Base 283h (syn0), V.35 interface. Only one single-port board is supported in a NetBlazer.
- **SYN*xxx* dual-port board:** syn10/syn11 (switches set to F0h). The interface daughter board types (RS-449, RS-530, V.35, and RS-232) are specified at time of initial order and are supplied with mating cables. Up to five dual-port synchronous boards can be installed in a NetBlazer 40 and up to two in a NetBlazer ST.

If your specific requirements involve a configuration other than the factory default settings identified above, or if you are installing more than one synchronous board, it is necessary to change the setting on switch SW2 on the SYN*xxx* dual-port synchronous board.

Perform the following procedures that are applicable.

Opening the NetBlazer Case

Warning: *Make sure that the NetBlazer is not connected to an AC power outlet; then open the NetBlazer case by performing the following steps:*

1. Using a Phillips screwdriver, remove the screws on the rear or side of the NetBlazer top cover, as shown in Figure 3-1 of your *NetBlazer ST* or *40 Installation Guide*.
2. Slide the top cover back and lift it off the NetBlazer.

This board is assigned to I/O base address 283h. Because the NetBlazer can only support one board of this type, this address cannot be changed. No further configuration is necessary unless you need to change the interface type from V.35 to RS-232 or RS-422/RS-449. This change is accomplished by moving a series of header plugs containing jumpers into different sockets. Figure 3-1 shows the factory default configuration of this board.

Caution: *The synchronous board is sensitive to static electricity. Observe ESD handling precautions and discharge any static on your body by touching an unpainted surface on the NetBlazer's frame before inserting the board into the NetBlazer.*

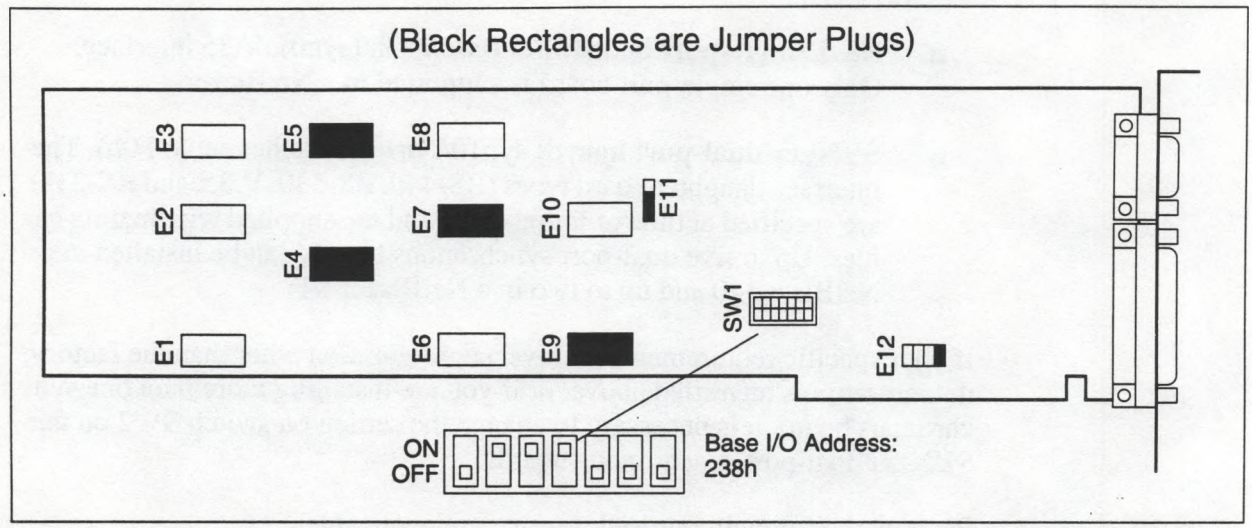


Figure 3-1. Single-Port Synchronous Board V.35 Configuration (Default)

V.35

The single-port synchronous interface board (along with a companion cable) is shipped from the factory configured to connect to a data service unit/channel switching unit (DSU/CSU) using a V.35 interface. If this matches your requirements, skip ahead to the next option.

RS-232 or RS-422/RS-449

If you have a DSU/CSU that uses an RS-232 or RS-422/RS-449 interface, you must obtain the appropriate cable and reconfigure the synchronous interface board by moving the four jumper plugs. If you are connecting to an ISDN TA (terminal adapter), contact Telebit Technical Support (1-800-TELEBIT or 408-734-5200) for a current list of compatible TAs.

Referring to Figure 3-2 for an RS-232 interface or Figure 3-3 for an RS-422/RS-449 interface, perform the following steps to configure the single-port synchronous interface board for an RS-232 or RS-422/RS-449 interface.

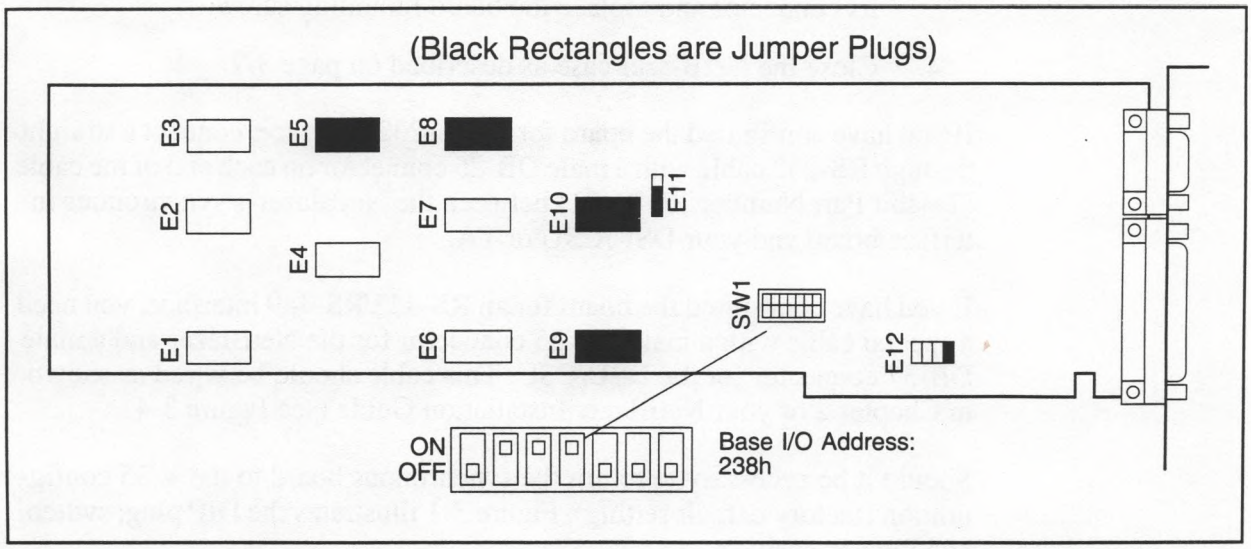


Figure 3-2. Single-Port Synchronous Board RS-232 Interface Configuration

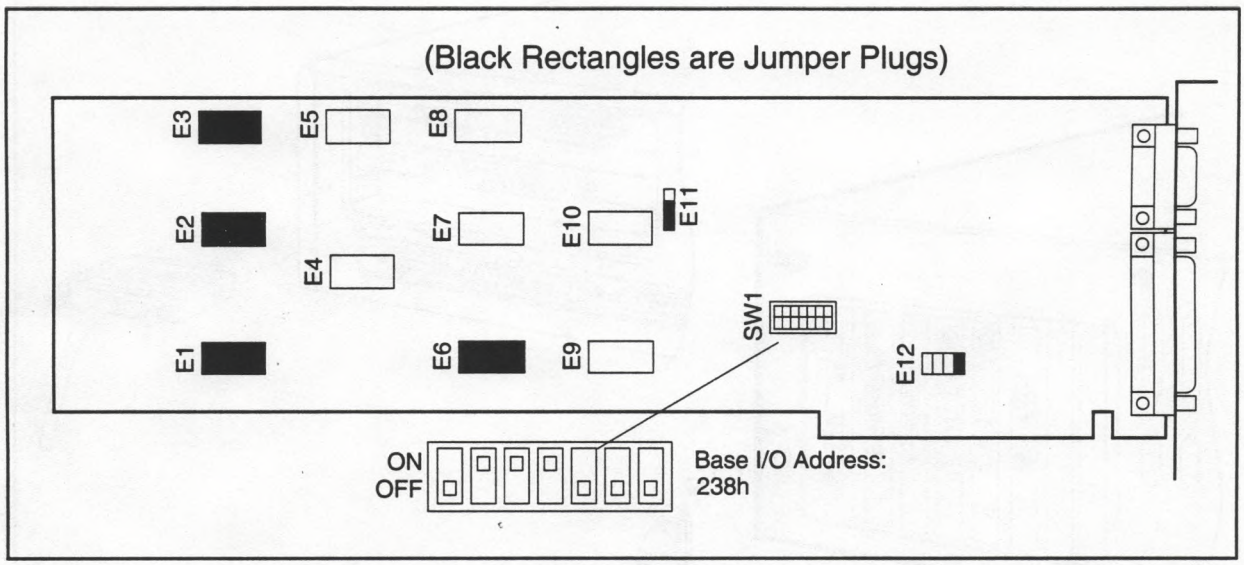


Figure 3-3. Single-Port Synchronous Board RS-422/449 Interface Configuration

1. Using a small flat-blade screwdriver or similar object, gently pry one end of the header plug up from its socket as illustrated by the highlighted (black) rectangles in the figures above. Repeat this at the other end of the header plug until the plug can be pulled straight out of the socket.

2. Verify that none of the pins on the plug has been bent, and place the plug over its new socket location.

3. Carefully guide the synchronous interface board into its slot so that the board's edge connector is aligned with the slot connector and the cable connectors extend through the slot opening. Make sure that all the pins on the plug are properly aligned with the socket, then firmly press on the top edge of the board so that it is securely mated with its connector and replace the board mounting screw.

4. Close the NetBlazer case as described on page 3-7.

If you have configured the board for an RS-232 interface, connect a straight-through RS-232 cable with a male DB-25 connector on each end of the cable (Telebit Part Number 12105-01) between the NetBlazer's synchronous interface board and your DSU/CSU or TA.

If you have configured the board for an RS-422/RS-449 interface, you need a special cable with a male DB-25 connector for the NetBlazer and a male DB-37 connector for the DSU/CSU. This cable should be wired as shown in Chapter 2 of your NetBlazer Installation Guide (see Figure 3-4).

Should it be necessary to return the synchronous board to the V.35 configuration (factory default setting), Figure 3-1 illustrates the DIP plug, switch, and jumper positions.

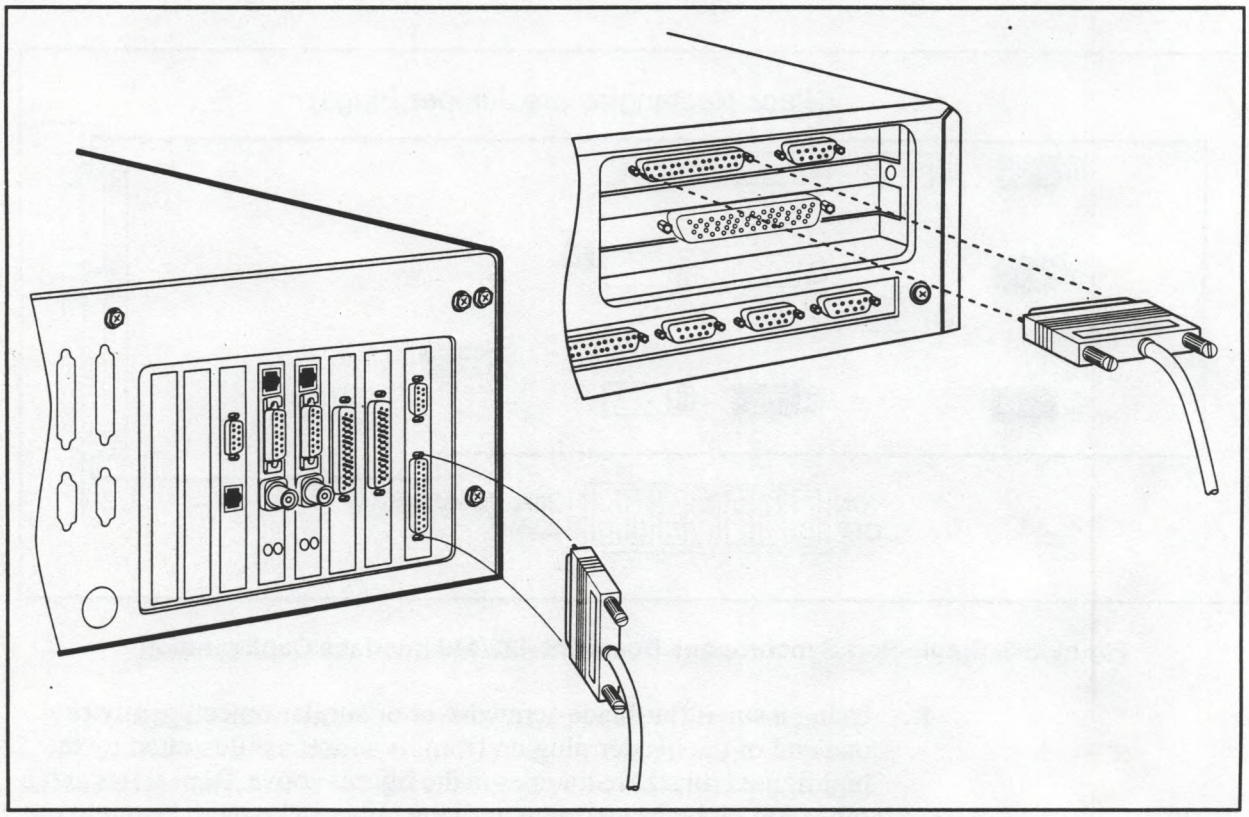


Figure 3-4. Connecting to the Single-Port Synchronous Board

The SYN*xxx* dual-port boards are assigned in the following group pairs:

- syn10 and syn11
- syn20 and syn21
- syn30 and syn31
- syn40 and syn41
- syn50 and syn51

Up to five SYN*xxx* dual-port synchronous boards can be installed in a NetBlazer. The *xxx* portion of the model number defines the interface type (i.e., SYN530 is a dual-port synchronous board with an RS-530 interface). The interface types (RS-530, V.35, RS-449, and RS-232) are specified at time of initial order and are supplied with mating cables.

Notes:

1. *Interface daughter boards must be of the same type and cannot be mixed on a dual-port synchronous board.*
2. *Interface cables are shipped with their respective daughter boards and are prewired for the interface type. Warning labels are provided on the daughter boards and interface cables clearly identifying their types.*
3. *Both RS-449 cables and RS-530 cables use the same daughter board.*
4. *The use of Port A is recommended for a high speed (T1 or E1) link. Port B is limited to 128-Kbps operation.*

Warning: *Be certain that the correct cable type is used with the corresponding daughter board. Plugging these cables into daughter boards of a different interface type can result in damage to the daughter board and/or connecting equipment.*

Table 3-1 summarizes the dual-port synchronous board models, their respective daughter board interface types, and mating cables.

Table 3-1. Interface Types

Dual-Port Synchronous Board Model	Interface Type	Cable
SYN449	RS-449	12720-01
SYN530	RS-530	13203-01
SYN35	V.35	12722-01
SYN232	RS-232	12721-01

Caution: *The main synchronous board and the daughter boards are sensitive to static electricity. Observe ESD handling precautions and discharge any static on your body by touching an unpainted surface of the NetBlazer's frame before inserting these boards into the NetBlazer.*

Note: *Only the V.35 interface daughter board contains a jumper. Be sure it is positioned on the two upper pins as shown in Figure 3-5.*

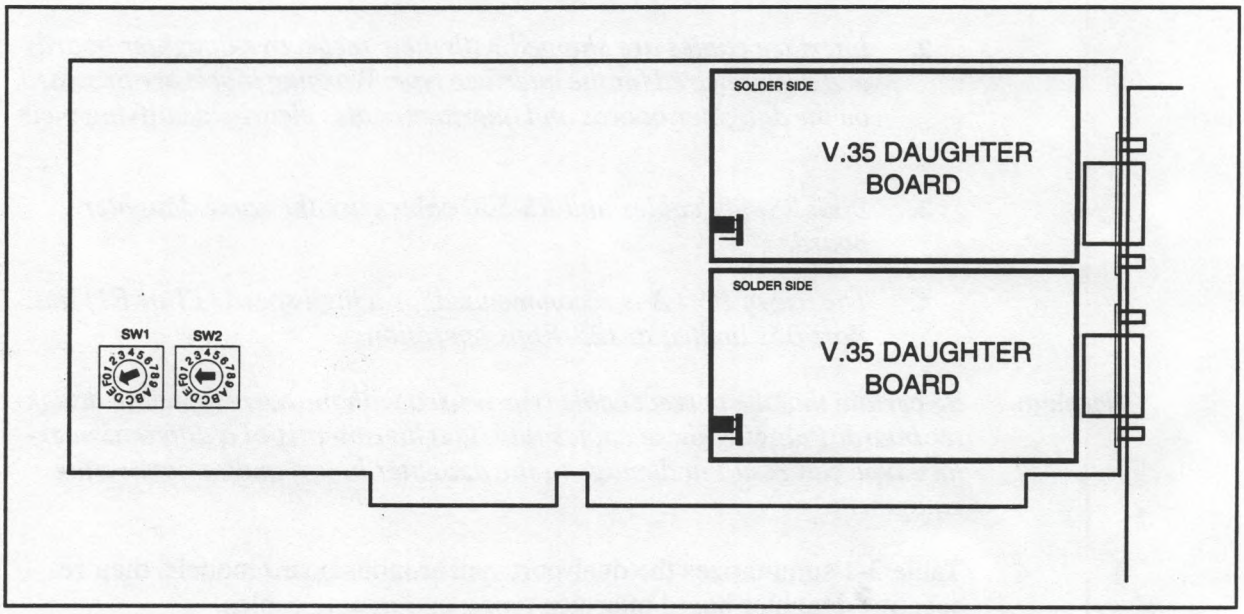


Figure 3-5. V.35 Daughter Board Jumper Position

Setting Switches on the Dual-Port Synchronous Board

As shipped from the factory, the SYN*xxx* dual-port synchronous boards are preset to syn10 and syn11 (switches set to F0h). If you are adding more than one synchronous board to your NetBlazer, determine the required setting of SW2 on the main board (see Figure 3-5).

Table 3-2. Synchronous Board Base I/O Address Assignments

Synchronous Board	Switch Setting (SW2)
syn0*	Reserved for single-port synchronous board
syn10, syn11	F0
syn20, syn21	F2
syn30, syn31	F4
syn40, syn41	F6
syn50, syn51	F8

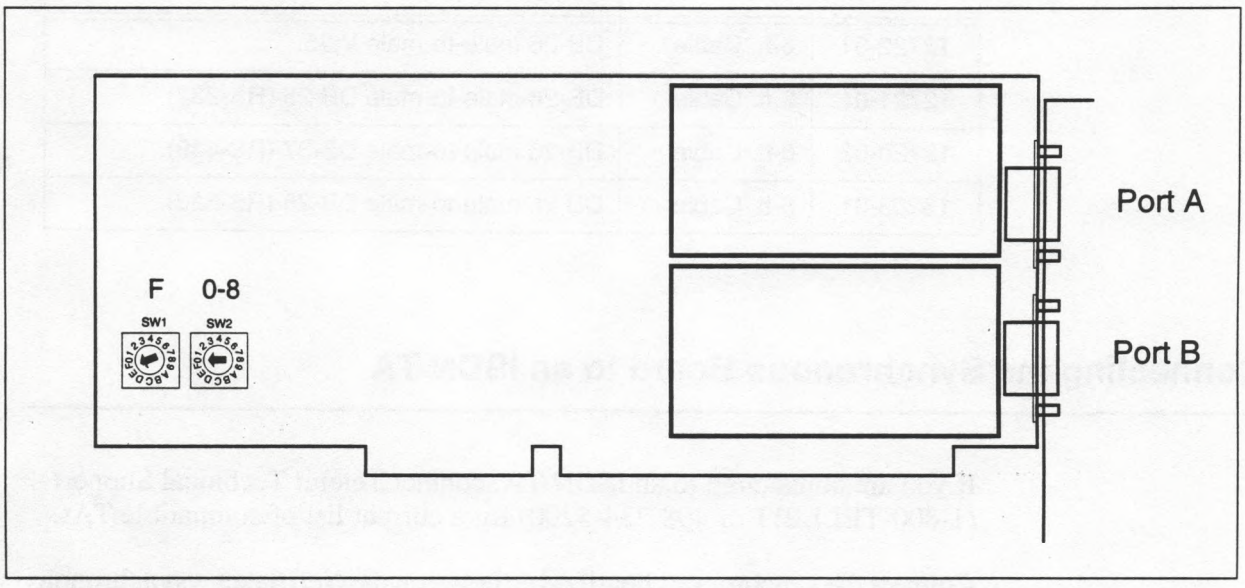


Figure 3-6. Dual-Port Synchronous Board Address Switch Location

Closing the NetBlazer Case

1. Close the NetBlazer case as described in Chapter 3 of your *NetBlazer ST* or *40 Installation Guide*.
2. Apply the appropriate stick-on labels (supplied with the NetBlazer) to the synchronous ports.

3. Connect the AC power cord supplied with your NetBlazer between the power cord connector on the back of the NetBlazer and an AC outlet.

Connecting the Synchronous Board to a DSU/CSU

Connect the synchronous board to DSU/CSU using the appropriate cable. Secure the cable end connectors to the board with the captive thumb screws.

Note: *The use of Port A is recommended for a high speed (T1 or E1) link.*

Table 3-3 provides additional detail about the Telebit cables available for the various interface types.

Table 3-3. Synchronous Cables

Part No.	Item	Description
12722-01	6-ft. Cable	DB-26 male-to-male V.35.
12721-01	6-ft. Cable	DB-26 male-to-male DB-25 (RS-232).
12720-03	6-ft. Cable	DB-26 male-to-male DB-37 (RS-449).
13203-01	6-ft. Cable	DB-26 male-to-male DB-25 (RS-530).

Connecting the Synchronous Board to an ISDN TA

If you are connecting to an ISDN TA, contact Telebit Technical Support (1-800-TELEBIT or 408-734-5200) for a current list of compatible TAs.

Connect the synchronous board cable between the NetBlazer's synchronous port and the ISDN TA. Refer to the instructions provided with your TA as required.

Asynchronous Board Installation 4

This document provides instructions for installing two models of Telebit multiport asynchronous boards in a NetBlazer: the NM8 and the ASYN8. The ASYN8 board supersedes the NM8 asynchronous board and provides up to 24 serial interface ports in banks of 8 ports. Expansion is accomplished by adding model ASYN8+ modular terminal adapter (MTA) modules.

NM8 Multiport Board

If you are adding an NM8 multiport board to your NetBlazer to support external modems, perform the following steps:

1. Set DIP switches DS1 and DS2 to the settings shown in Figure 4-1.

Caution: *The NM8 multiport board is sensitive to static electricity. Observe ESD handling precautions and discharge any static on your body by touching an unpainted surface of the NetBlazer's frame* before *inserting the board.*

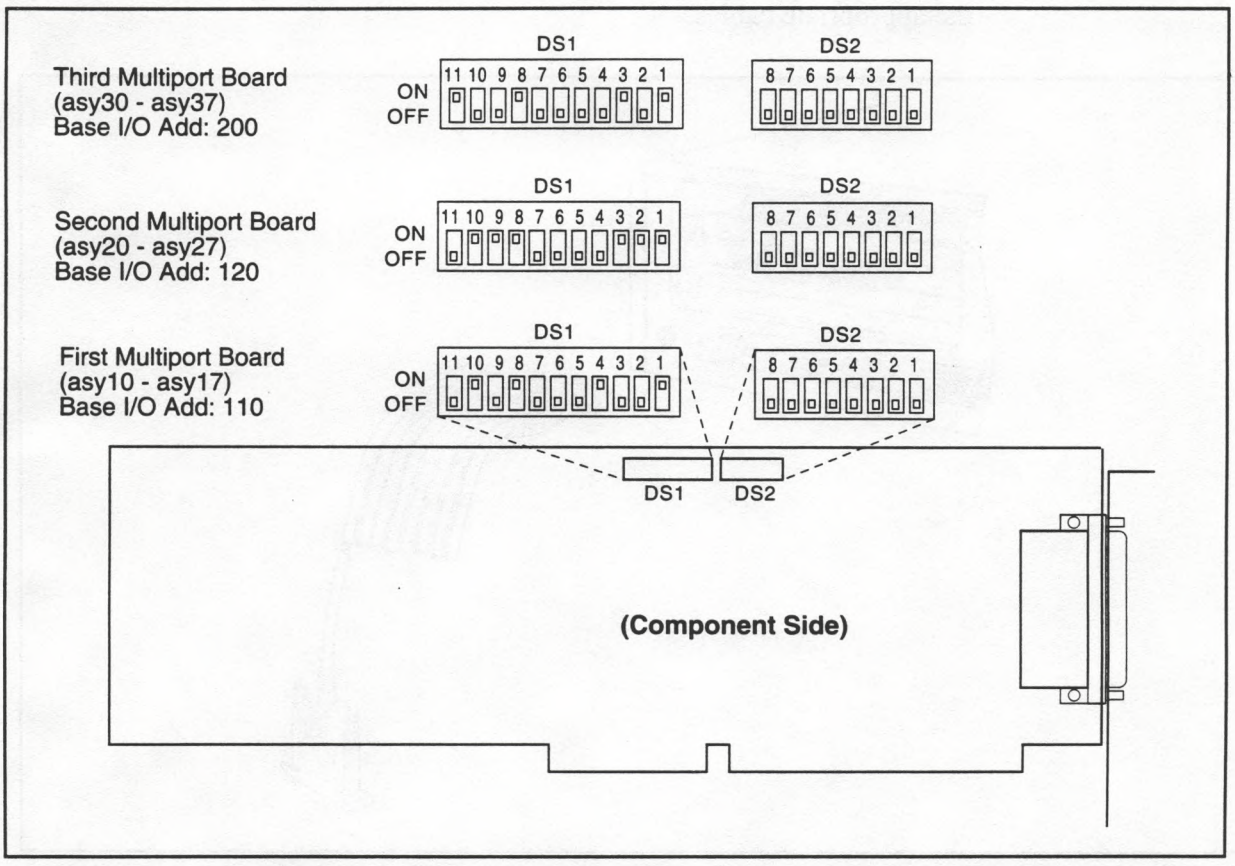


Figure 4-1. NM8 Multiport Board Switch Settings

2. Carefully guide the multiport board into its slot in the NetBlazer so that the board's edge connector is aligned with the slot connector and the cable connector extends through the slot opening.

3. Firmly press on the top edge of the board so that it is securely mated with its connector, and replace the board mounting screw.

External Modems

You can connect up to 26 standalone or rackmount modems to a NetBlazer 40 containing two standard asynchronous ports and three multiport expansion boards (18 modems on a NetBlazer ST).

Notes:

1. *4 Mbytes of system DRAM are required when using two or three multiport boards. Contact Telebit Technical Support at 1-800-TELEBIT (408 734-5200) for details.*

2. *Telebit recommends that you use shielded cables.*

A cable is provided by Telebit for each multiport expansion board installed in your system. To connect a modem to either of the two standard asynchronous ports, you need a shielded RS-232 cable for each port. Refer to Table 4-1 in this section and the Modem Requirements section in Chapter 2 of your *NetBlazer ST or 40 Installation Guide* for information on acquiring the appropriate cables.

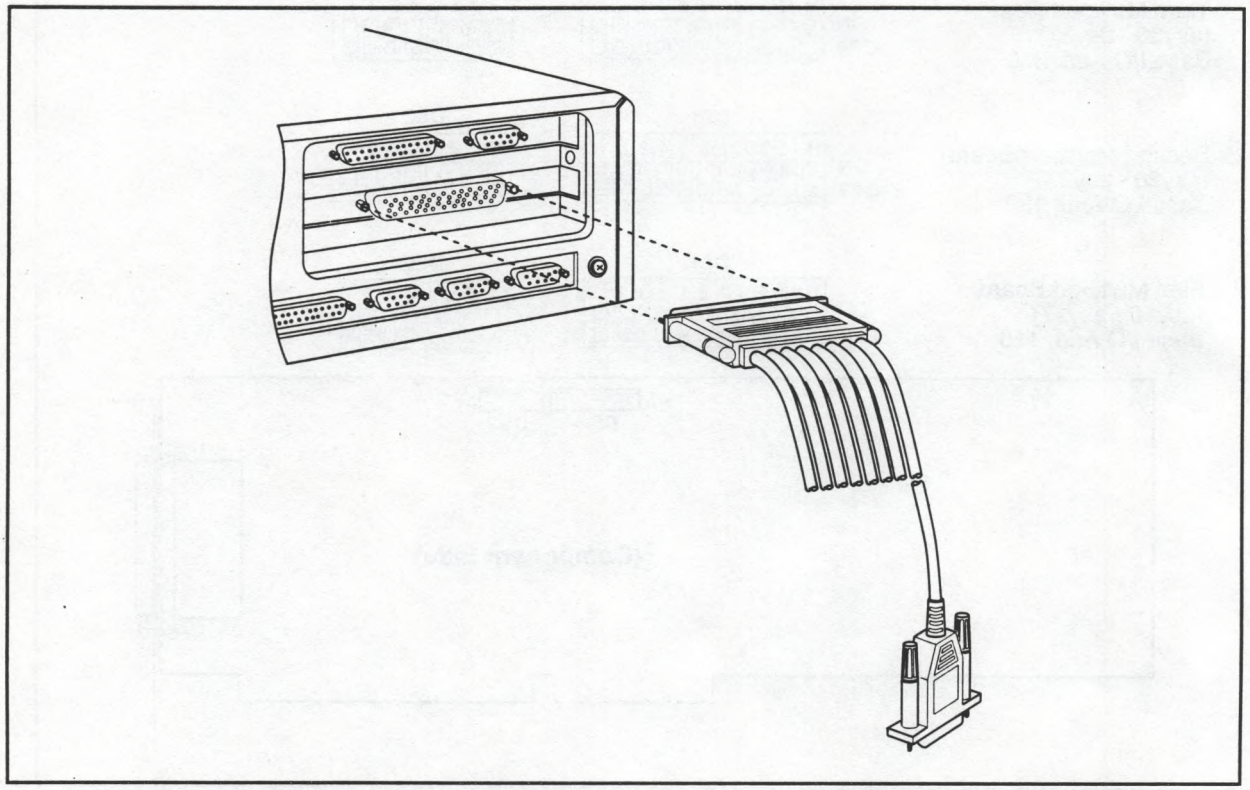


Figure 4-2. Multiport Cable Connection

Note: *Modems should be connected to multiport expansion board ports before using the two standard asynchronous ports for modems, because the multiport expansion boards have their own controller for better performance under heavy loading.*

To connect the multiport expansion cable to the NetBlazer, connect the large 78-pin connector to the multiport board connector on the back of the NetBlazer, as illustrated in Figure 4-2. Connect each of the eight RS-232 cable connectors to the RS-232 connector on the back of a standalone modem or to one of the RS-232 connectors on the back of a rackmount modem chassis.

Refer to the manual supplied with your modem for further instructions on how to install and configure the modem.

ASYN8 Multiport Asynchronous Board

Factory Default Option Settings

As shipped from the factory, the ASYN8 asynchronous board is preset to I/O base address E0h. Because this board supports 24 ports, it is not necessary to change this switch setting.

Notes:

1. *4 Mbytes of system DRAM are recommended when using more than eight ports. Contact Telebit Technical Support at 1-800-TELEBIT or (408) 734-5200 for details.*
2. *Telebit recommends that you use shielded cables to connect to modems.*

Opening the NetBlazer Case

Warning: *Make sure that the NetBlazer is not connected to an AC power outlet; then open the NetBlazer case by performing the following steps:*

1. Using a phillips screwdriver, remove the screws on rear or sides of the NetBlazer top cover as shown in Figure 3-1 of your *NetBlazer ST or 40 Installation Guide*.
2. Slide the top cover back and lift it off the NetBlazer.

Caution: *The ASYN8 asynchronous board is sensitive to static electricity. Observe ESD handling precautions and discharge any static on your body by touching the NetBlazer's frame before inserting the board.*

Installing the ASYN8 Asynchronous Board

After verifying that the setting of the two switches are E0 and the jumper to the right of the switches is in the '0' position, install the ASYN8 board. Carefully guide the board into its slot (as shown in your *NetBlazer Installation Guide*) so that the board's edge connector is aligned with the slot connector and the 37-pin connector extends through the slot opening. Then firmly press on the top edge of the board until it is securely mated with its connector. Replace the mounting screw.

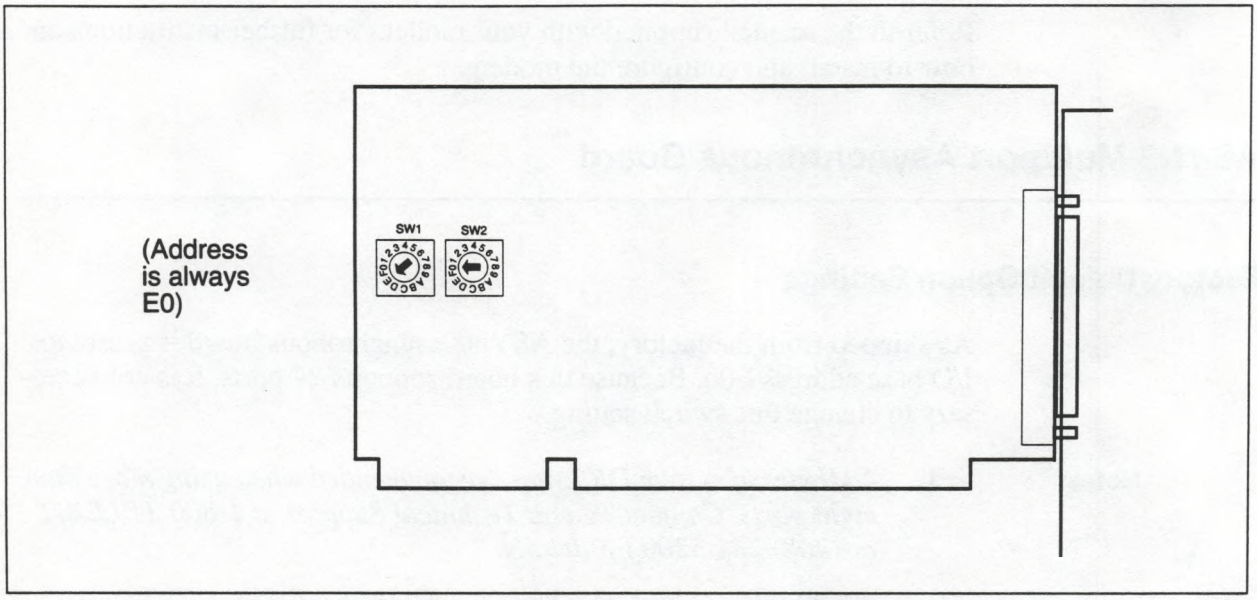


Figure 4-3. ASYN8 Asynchronous Board Switches

Closing the NetBlazer Case

Close the NetBlazer case as described in Chapter 3 of your *NetBlazer ST or 40 Installation Guide*. Connect the AC power cord supplied with your NetBlazer between the power cord connector on the back of the NetBlazer and an AC outlet.

Configuring the MTAs

The ASYN8 board is furnished with one 8-port MTA. This MTA provides a block of 8 DB-25 male connector RS-232 breakout ports for the ASYN8 asynchronous board. Additional MTAs (ASYN8+) can be coupled to provide 24 ports for connection to external modems or other serial devices.

If you are adding MTAs, it is necessary to disassemble the MTAs and couple them together. Perform the following steps:

1. Using a flat-blade screwdriver, gently pry up each end of the ribbed trim strip on the top of the MTA until it unsnaps. Remove the trim strip and set it aside.

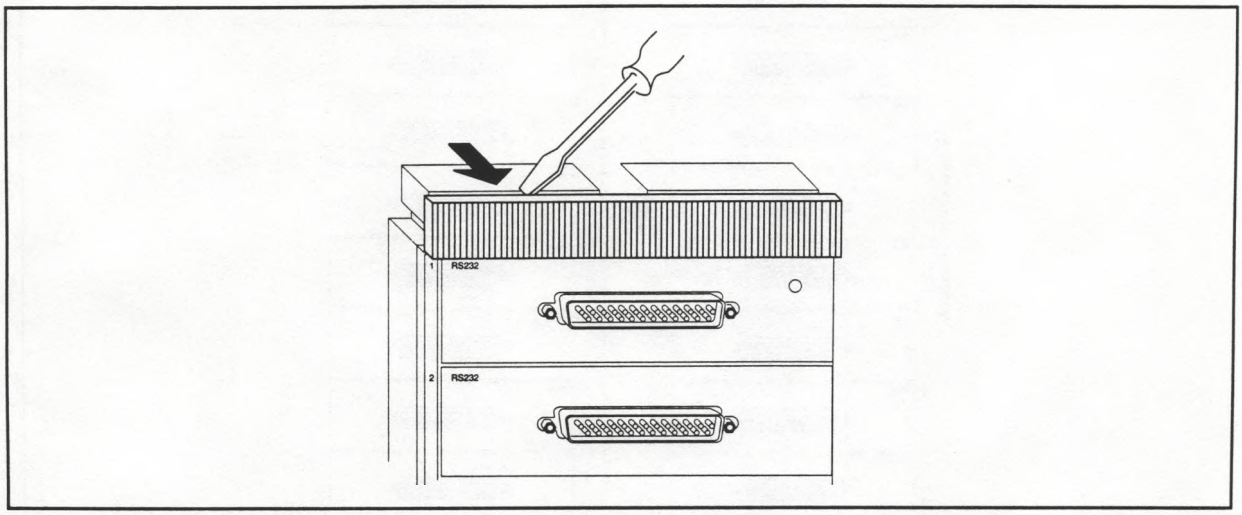


Figure 4-4. Trim Removal

2. Repeat the procedure for the strip on the bottom edge of the MTA.
3. Unsnap the two rectangular lower panels (one on each end of the MTA) and set them aside.

4. Orient the MTAs alongside of each other and plug them together as illustrated in Figure 4-5.

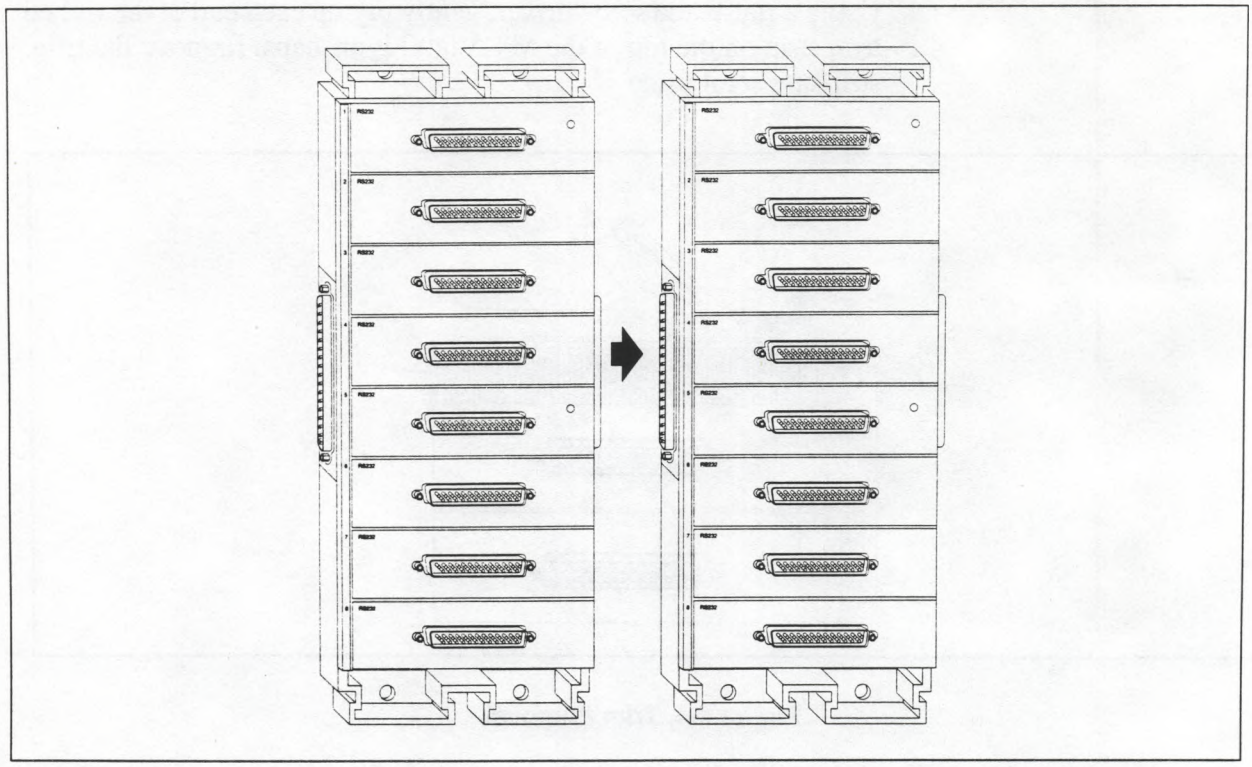


Figure 4-5. MTA Connection

5. Lock the MTAs together using the lower rectangular panels as interlocking brackets as illustrated in Figure 4-6.

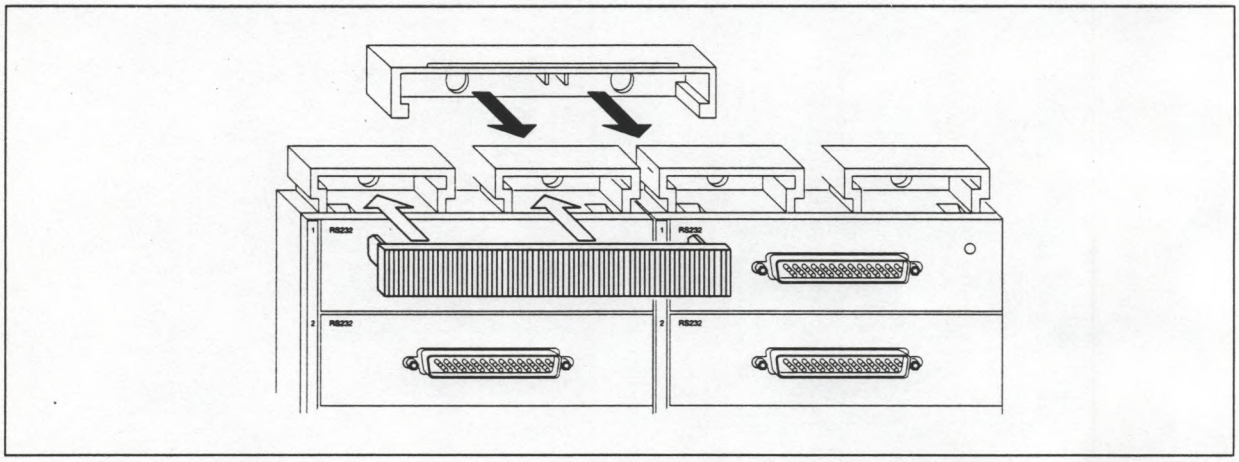


Figure 4-6. Interlocking the Modules

6. Replace the trim strips on both ends of the MTAs.

Connecting the ASYN8 Board to the MTA

Warning: *The NetBlazer power must be turned off before connecting the cable to the MTAs.*

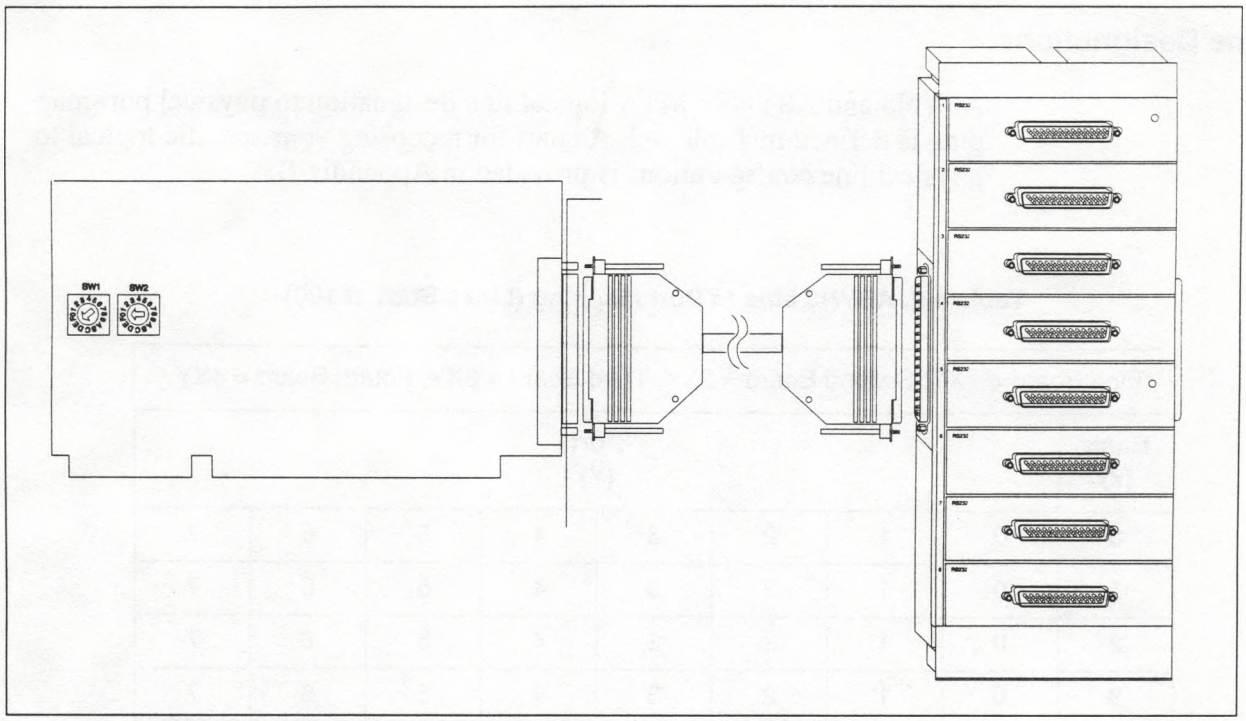


Figure 4-7. Connecting the Asynchronous Board to the MTA

Connect the 37-pin cable furnished with the ASYN8 asynchronous board to the MTA as illustrated in Figure 4-7. Secure the connector to the board with its captive thumbscrews.

Connecting to the ASYN8 MTA RS-232 Ports

Referring to Table 4-1, select the appropriate cable to connect the MTA ports to your modems or serial devices. Telebit recommends that you use shielded cables.

Table 4-1. Cable Descriptions

Part No.	Item	Description
12103-01	6-ft. Cable	DB-25 male to DB-25 female, null modem.
12104-01	6-ft. Cable	DB-25 male to DB-9 female, straight through.
12105-01	6-ft. Cable	DB-25 male to DB-25 female, straight through.
12724-01	6-ft. Cable	DB-25 male to DB-9 female, null modem.

MTA Rackmount Adapter

A special rack adapter kit that mounts four MTAs and their external power supply to a standard 19-inch rack is planned. Call your Telebit sales representative for availability details.

Line Designations

ASYN8 and ASYN8+ MTA logical line designation to physical port mapping is defined in Table 4-2. A chart for recording your specific logical to physical line configurations is provided in Appendix B.

Table 4-2. ASYN8 Line to Port Mapping (Lines Start at 100)

First Board = 1XY; Second Board = 2XY; Third Board = 3XY; Fourth Board = 4XY.								
Bank (x)	**Port (Y)**							
0	0	1	2	3	4	5	6	7
1	0	1	2	3	4	5	6	7
2	0	1	2	3	4	5	6	7
3	0	1	2	3	4	5	6	7

Interface Board Pinouts A

The following pinout information is provided as a convenience to those who wish to fabricate their own cables and for general reference.

DB-15 Connector

Pin	Description
1	Control in circuit shield (Shield)
2	Control in circuit A (Collision +)
3	Data out circuit A (Transmit +)
4	Data in circuit shield
5	Data in circuit A (Receive +)
6	Voltage common (Power-Gnd)
7	Control out circuit A
8	Control out circuit shield
9	Control in circuit B (Collision -)
10	Data out circuit B (Transmit -)
11	Data out circuit shield
12	Data in circuit B (Collision -)
13	Voltage plus (Power +12V)
14	Voltage shield
15	Control out circuit B
Shell	Protective ground

RJ-45 Socket

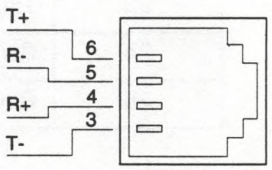
Pin	Description
1	Data Out (+)
2	Data Out (-)
3	Data In (+)
4	NC
5	NC
6	Data In (-)
7	NC
8	NC

NTR Token Ring Board Pinouts

DB-9

Pin	Description
1	Receive (+)
2	GND
3	+5V
4	GND
5	Transmit (-)
6	Receive (-)
7	GND
8	GND
9	Transmit (+)

RJ-45

Pin	Description	Diagram
1	NC	
2	NC	
3	Transmit (-)	
4	Receive (+)	
5	Receive (-)	
6	Transmit (+)	
7	NC	
8	NC	

NS1 (Single-Port) Synchronous Board Pinouts

DB-25

Because the single-port synchronous board remaps these pinouts for V.35, RS-422, or RS-449 through a DIP switch and various DIP plugs, refer to Figures 2-1 and 2-2 in Chapter 2 for these pinouts. Standard V.35 configuration pinouts are:

Pin	Description
4	RTS
5	CTS
6	DSR
7	GND
8	DCD
10	RDB/Rx (+)
11	RDA/Rx (-)
12	TDB/Tx (+)
13	TDA/Tx (-)
20	DTR
21	TxCB/TxC (+)
22	RI
23	TxCA/TxC (-)
24	RxCB/RxC (+)
25	RxCA/RxC (-)

DB-9

The NetBlazer does not support the DB-9 connector.

SYN*xxx* (Dual-Port) Synchronous Board Pinouts

The dual-port synchronous board is furnished with cables designed to mate specifically with their respective interface daughter boards. The use of any other cables could cause damage to the equipment and therefore is not recommended.

Note: *The use of shielded cables is recommended for all serial connections.*

NM8 Multiport Asynchronous Board Octopus Cable Pinouts

Pinouts at the end of each DB-25 connector:

Pin	Description
2	Transmit Data (TxD)
3	Receive Data (RxD)
4	Request to Send (RTS)
5	Clear to Send (CTS)
6	Data Set Ready (DSR)
7	Signal Ground
8	Carrier Detect (CD)
20	Data Terminal Ready (DTR)
22	Ring Indicator (RI)

ASYN8 Multiport Asynchronous Board MTA Cable Pinouts

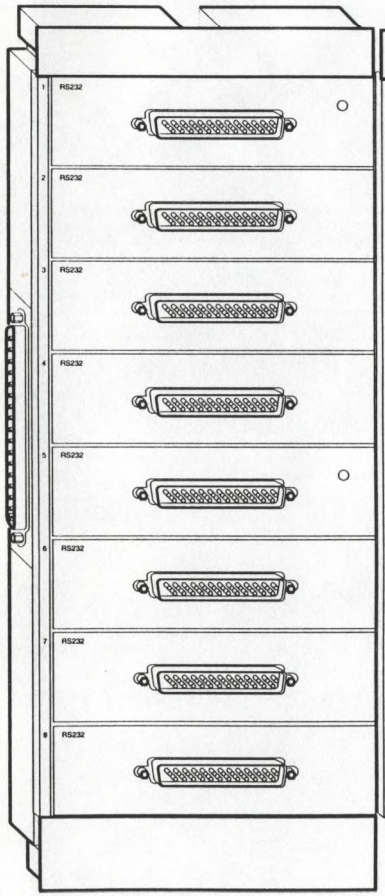
A special cable connecting the ASYN8 board to its mating MTA is supplied with the board and MTA. The following table lists the pinouts of the eight DB-25 male connectors on the MTA.

Pin	Description
1	Chassis GND
2	Transmit Data (TxD)
3	Receive Data (RxD)
4	Request to Send (RTS)
5	Clear to Send (CTS)
6	Data Set Ready (DSR)
7	Signal Ground
8	Carrier Detect (CD)
20	Data Terminal Ready (DTR)

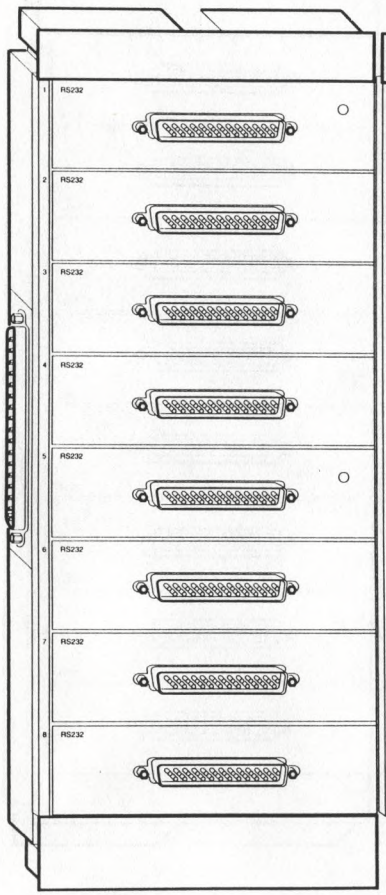
MTA Line Assignment Record B

The following diagram/table is provided as a convenience in documenting your specific asyn logical to physical line configurations when using the ASYN8 asynchronous board and its MTAs.

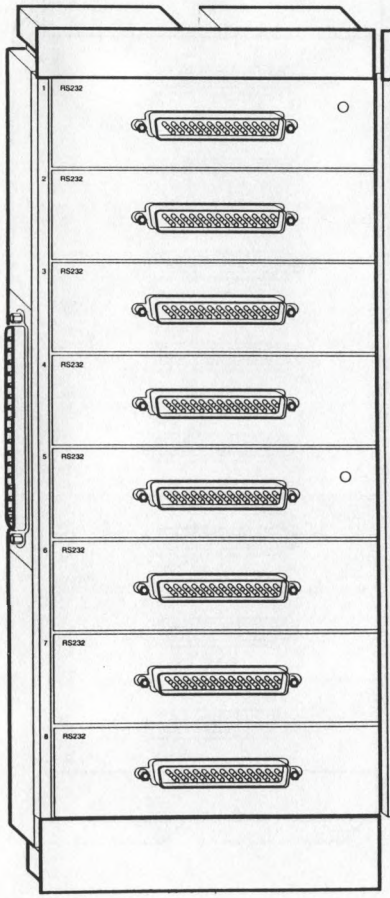
Photocopy the illustration as necessary. You may also wish to keep a copy physically with the MTA. A plastic page protector facilitates easy attachment to the cabinet or to the cables.



MTA 1	MTA 2	MTA 3	MTA 4
0	0	0	0
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7



MTA 1	MTA 2	MTA 3	MTA 4
0	0	0	0
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7



MTA 1	MTA 2	MTA 3	MTA 4
0	0	0	0
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7

Other Ethernet Board Configurations C

The following information is furnished to provide continuity in documentation of previous versions of Telebit Ethernet boards. Note that these boards have been superseded by the NE1 Ethernet board.

First-Generation Ethernet Board (WD8013)

This Ethernet board provides both thin Ethernet (BNC) and thick Ethernet (AUI) connections to a local area network. The board is preset at the factory for connection to thin Ethernet media. If you plan to use the AUI media type, you must change the W3 jumper to activate this connector as shown in Figure C-1.

Ethernet board interface assignment (en0, en1, and en2) jumpers are illustrated in Figure C-2.

Caution: *The Ethernet board is sensitive to static electricity. Observe ESD handling precautions and discharge any static on your body by touching an unpainted surface of the NetBlazer's frame before inserting the board.*

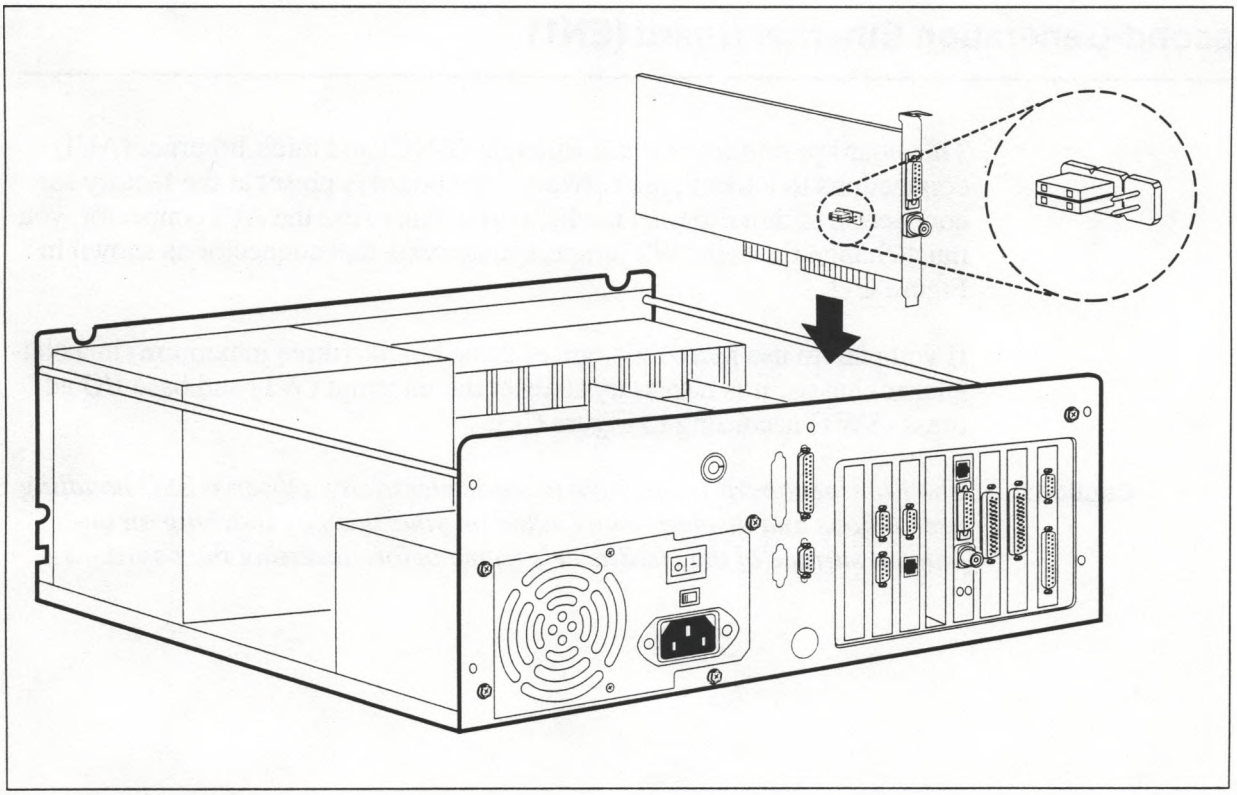
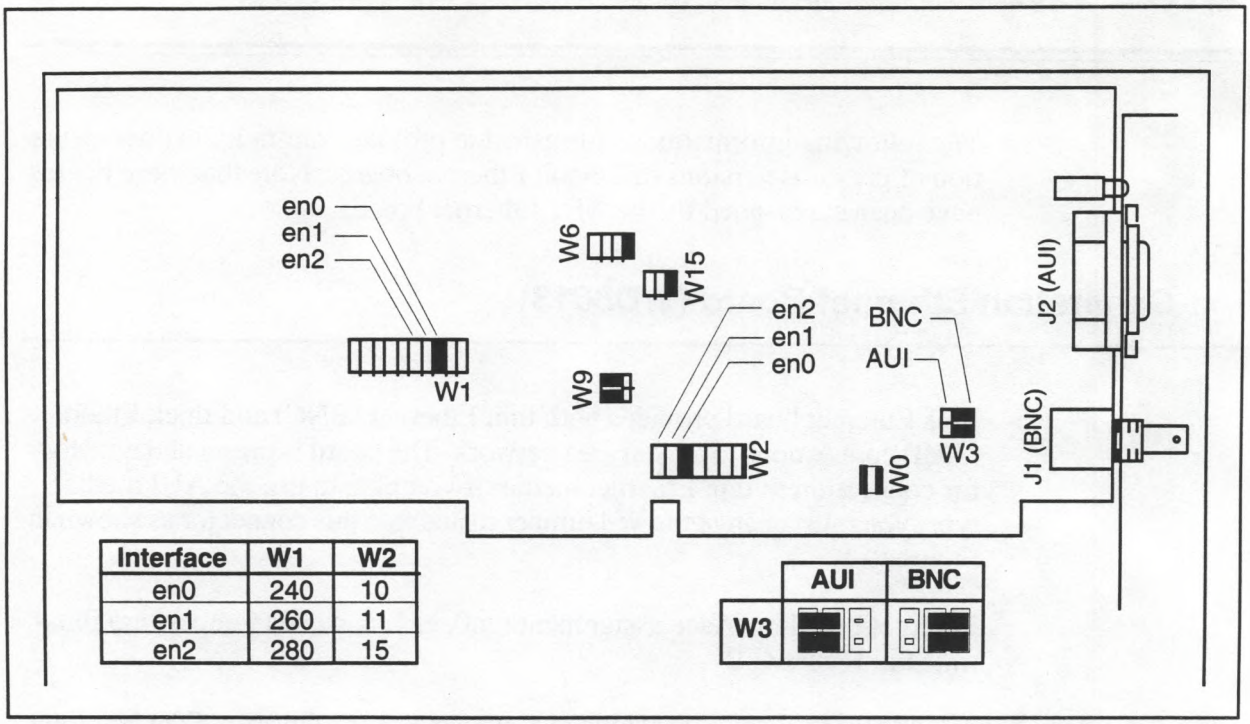


Figure C-1. First-Generation Ethernet Board Media Type Jumper Locations



Interface	W1	W2
en0	240	10
en1	260	11
en2	280	15

Figure C-2. WD8013 Ethernet Interface Assignment Jumpers

Second-Generation Ethernet Board (EN1)

This board provides both thin Ethernet (BNC) and thick Ethernet (AUI) connections to a local area network. The board is preset at the factory for connection to thin Ethernet media. If you plan to use the AUI connector, you must change the eight W2 jumpers to activate this connector as shown in Figure C-2.

If you plan to use more than one of these boards (three maximum) in a NetBlazer chassis, it is necessary to reset the interrupt (W1) and base I/O address (SW1) according to Figure C-3.

Caution: *The Ethernet board is sensitive to static electricity. Observe ESD handling precautions and discharge any static on your body by touching an unpainted surface of the NetBlazer's frame before inserting the board.*

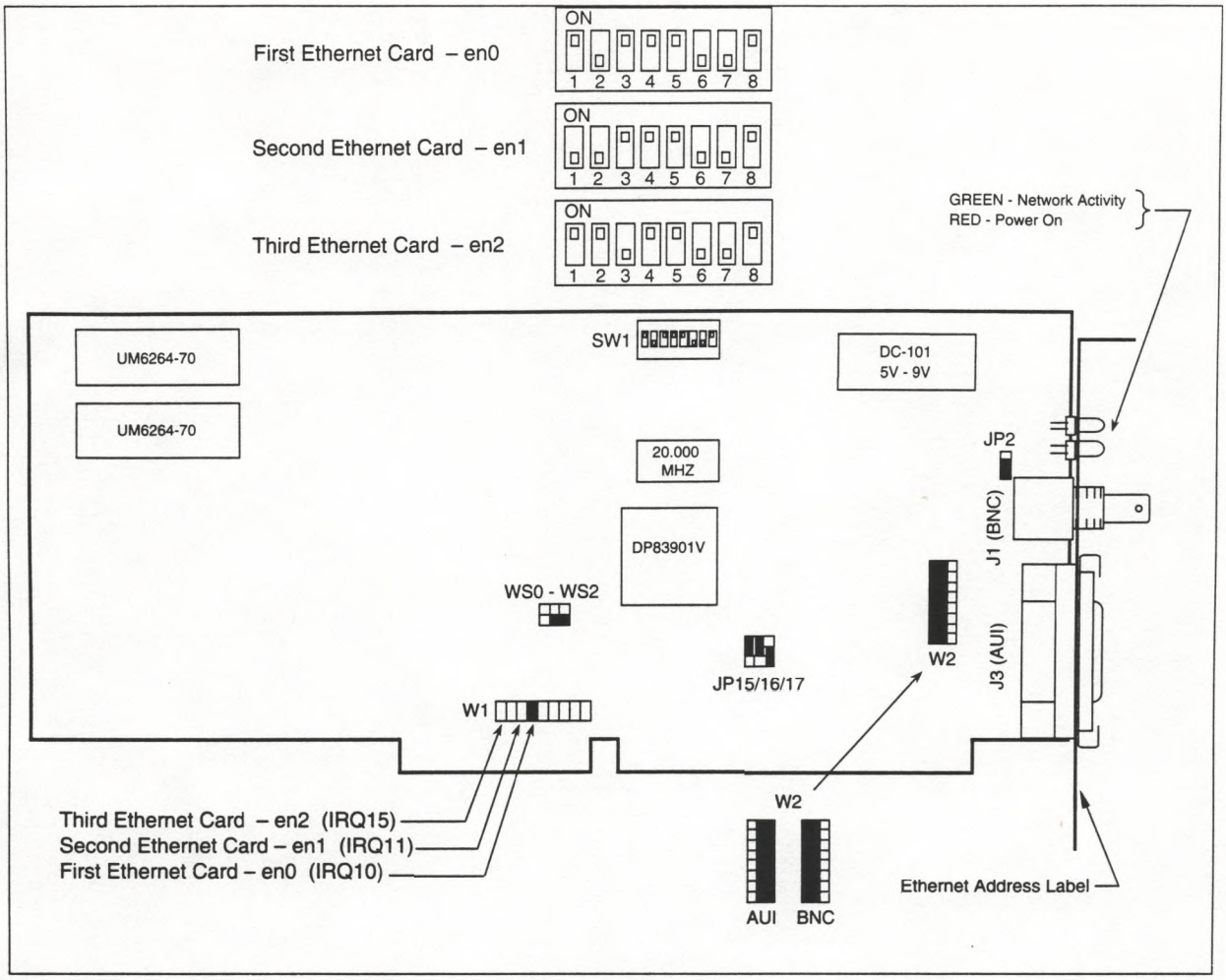


Figure C-3. Second-Generation Ethernet Board Jumper Locations

Configuration Guide

90272-01 3/23/93

Trademarks

Telebit, NetBlazer, and TrailBlazer are trademarks of Telebit Corporation.

Telebit gratefully acknowledges the following additional copyrights:

- Apple and AppleTalk are registered trademarks of Apple Computer, Inc.
- Novell and NetWare are registered trademarks of Novell, Inc.
- UNIX is a registered trademark of AT&T Bell Laboratories.
- TCL is copyrighted by the University of California, Berkeley (unrestricted redistribution).

Other brands or product names are trademarks or registered trademarks of their respective holders.

Software Copyright Notice

This product contains software which has been copyrighted by Telebit Corporation, Sunnyvale, CA. All rights are reserved.

PLEASE READ THIS NOTICE CAREFULLY BEFORE USING THE NETBLAZER. BY USING THE SOFTWARE, YOU ARE AGREEING TO THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, PROMPTLY RETURN THE UNUSED SOFTWARE TO THE PLACE OF PURCHASE AND YOUR MONEY WILL BE REFUNDED.

1. License. The NetBlazer software (the "Software") and related documentation are licensed to you by Telebit Corporation. You own the disk on which the Software is recorded but Telebit retains title to the Software. This License allows you to use the Software on a single computer and to make one copy of the Software in machine-readable form for backup purposes and a reasonable number of copies of the following files for your remote access to your NetBlazer: PPPCFG.EXE, PPPCFG.MDM, PPPCFG.HLP, IPX.COM, COMPPP.EXE, IPXPPP.LAN, and WATCHPPP.EXE. You must reproduce on all such copies the copyright notice and any other proprietary legends that were on the original copy of the Software. You may transfer the Software, the backup copy and copy(s) for remote access of the Software, the related documentation and a copy of this License to another party provided the other party reads and agrees to accept the terms and conditions of this License.

2. Restrictions. The Software contains copyrighted material, trade secrets, and other proprietary information and in order to protect them you may not decompile, reverse engineer, disassemble or otherwise reduce the software to a human-perceivable form. You may not modify, network, rent, lease, loan, sell, distribute or create deriva-

tive works based upon the Software in whole or in part. Use, duplication, or disclosure of the Software by the U.S. Government is subject to restrictions as set forth in subdivision (b) (3) (ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013. Use, duplication, and disclosure by the governments of any other countries is subject to restrictions to similar applicable laws.

3. Termination. This License is effective until terminated. You may terminate this License at any time by destroying the Software and all copies thereof. This License will terminate immediately without notice from Telebit if you fail to comply with any provision of this License.

4. Limited Warranty on Media. Telebit warrants the disks on which the Software is recorded to be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date of purchase as evidenced by a copy of the receipt. Telebit's entire liability and your exclusive remedy will be replacement of the disk not meeting Telebit's limited warranty and which is returned to Telebit or a Telebit authorized representative with a copy of the receipt. Telebit will have no responsibility to replace a disk damaged by accident, abuse, or misapplication.

5. Disclaimer or Warranty on Software. You expressly acknowledge and agree that use of the Software is at your sole risk. The Software and related documentation are provided "AS IS" and without warranty of any kind and Telebit EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TELEBIT DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. FURTHERMORE, TELEBIT DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR RELATED DOCUMENTATION IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY TELEBIT OR A TELEBIT AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE SOFTWARE PROVE DEFECTIVE, YOU (AND NOT TELEBIT NOR A TELEBIT AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation of Liability.UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL TELEBIT BE LIABLE FOR ANY INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OR INABILITY TO USE THE SOFTWARE OR RELATED DOCUMENTATION, EVEN IF TELEBIT OR A TELEBIT AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THAT THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. In no event shall Telebit's total liability to you for all damages, losses, and causes of action whether in contract, tort (including negligence) or otherwise exceed the amount paid by you for the Software.

7. Controlling Law and Severability. This License shall be governed by and construed in accordance with the laws of the State of California, except that body of California law concerning conflicts of law. If for any reason a court of competent jurisdiction finds any provision of this License, or portion thereof, to be unenforceable, that provision of the License shall be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this License shall continue in full force and effect.

8. Complete Agreement. This License constitutes the entire agreement between the parties with respect to the use of the Software and related documentation, and supersedes all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter.

Copyright © 1993 Telebit Corporation.

Printed in U.S.A.

How to Use This Manual

This guide provides instructions for configuring the NetBlazer to the operational requirements of the network environment in which the NetBlazer will be used. It is intended as a general guide to the system administrator in performing both initial configuration and management activities.

This guide assumes that all NetBlazer hardware has been preconfigured and installed in the NetBlazer chassis, and that all cabling to the network and telephone lines has been completed. This manual includes the following information:

- Chapter 1, Introduction, provides an overview of the NetBlazer followed by a description of the various roles that the NetBlazer plays in a TCP/IP, IPX, or AppleTalk environment.
- Chapter 2, NetBlazer Interface Descriptions, describes how the NetBlazer uses LAN, dedicated serial line, and dynamic interfaces.
- Chapter 3, Getting Started, covers making a working copy of the NetBlazer System distribution diskette, and performing the initial log-on and setup of the NetBlazer. It also discusses how to plan a configuration.
- Chapter 4, IP Router Configuration, provides instructions on how to configure the NetBlazer to route IP packets between local networks.
- Chapter 5, Dedicated IP Interface Configuration, describes how to configure the NetBlazer to route IP packets between a local and remote site over a dedicated point-to-point link.
- Chapter 6, Dynamic IP Interface Configuration, provides instructions on how to configure the NetBlazer to route IP packets over a dynamic dial-up interface.
- Chapter 7, Using Auto-Routes, explains how to enable the local IP routing table to include routes to the remote site only when a dial-in connection is established from the remote site.
- Chapter 8, Using Proxy ARP, shows how to allow the NetBlazer to respond to ARP requests intended for another machine.
- Chapter 9, IP Packet Filtering, explains the use of the NetBlazer's IP filter commands to restrict IP packet routing to and from designated networks or host addresses through a particular interface.
- Chapter 10, Modem Server Configuration, describes how to set up the NetBlazer as a modem server which allows users on the IP network to telnet to the NetBlazer and establish a serial character mode connection with a remote system.

- Chapter 11, User IDs and Destination Groups, covers setting up the user ID records. These records are required for each user logging into the NetBlazer, be it through a telnet session or by calling in from a remote terminal.
- Chapter 12, Setting Up Callback Security, describes how to set up the NetBlazer to call back a remote user at a specified destination.
- Chapter 13, Setting Up a Raw TCP Link, describes how to establish a raw TCP connection from a host on the network to the modem or other asynchronous device attached to a NetBlazer line.
- Chapter 14, Network Management, describes how to bootp and manage the NetBlazer over a TCP/IP network.
- Chapter 15, IPX Configuration, provides instructions on how to configure the NetBlazer to route IPX packets between local networks and over a dynamic dial-up interface.
- Chapter 16, AppleTalk Configuration, explains how to configure the NetBlazer's AppleTalk protocol functions and features.
- NetBlazer file definitions are described in the Appendix.

Audience

This document is procedural guide to assist System Administrators in configuring the NetBlazer.

Related Documentation

Hardware installation of the NetBlazer products is detailed in the *NetBlazer Installation Guides*.

The *NetBlazer Command Reference* provides descriptions of all the NetBlazer's commands. Each command description shows the command format followed by an explanation of the command and its parameters.

NetBlazer Training

Telebit's Customer Services group offers excellent NetBlazer training on topics such as "Introduction to Internetworking and TCP/IP," and "NetBlazer Technical Training." These comprehensive courses combine easy-to-read training materials with insightful lecture and labs. For more information and class schedules, contact Telebit Education and Training Services at 1-800-TELEBIT.

Table of Contents

Trademarks i
Software Copyright Notice i

How to Use This Manual v
Audience vi
Related Documentation vi
NetBlazer Training vi

Table of Contents vii

1 Introduction 1-1
Functional Overview 1-1
The Roles of the NetBlazer 1-2
Using the NetBlazer as a Router 1-2
Using the NetBlazer as a Terminal Server 1-5
Using the NetBlazer as a Modem Server 1-6
Using the NetBlazer as an ARA Server 1-7

2 NetBlazer Interface Descriptions 2-1
LAN Interfaces 2-1
Routing IP Packets Through a LAN Interface 2-3
Routing IPX Packets Through a LAN Interface 2-3
Routing AppleTalk Packets Through a LAN Interface 2-4
Dedicated Serial Line Interfaces 2-4
Setting Up a Dedicated Interface Link 2-4
Setting Up a Dynamic Backup for a Dedicated PPP Interface 2-6
Dynamic Interfaces 2-7
Allowing Dial-Out Connections 2-8
Allowing Dial-In Connections 2-8
Three Methods to Set Up a Dynamic Interface 2-8
Choosing PPP or SLIP Framing 2-10
Routing Packets Through a Dynamic Interface 2-10
Setting Up a Synchronous Dynamic Interface 2-11

3 Getting Started 3-1
Overview 3-1
Customizing The STARTUP.CNF File 3-1
On-line Editing Steps 3-3
Using MS-DOS to Back Up the System Diskette 3-4
Using MS-DOS to Preconfigure the STARTUP.CNF File 3-4
Starting the NetBlazer and Logging in as Root 3-6
On an AppleTalk Network 3-6
Using an Administrator's Workstation 3-8

Using NetBlazer's Diskcopy to Back Up the System Diskette 3-8
Assigning a Host Name to the NetBlazer 3-9
Setting the Current Date and Time 3-9
Setting the Root Password 3-10
Saving the NetBlazer System Configuration 3-11
What's Next 3-11

4 IP Router Configuration 4-1
Assigning a Global IP Address to the NetBlazer 4-2
Assigning an IP Address to Each LAN Interface 4-2
Configuring the NetBlazer to Use RIP and/or Static Routes 4-3
Using RIP (Routing Information Protocol) 4-4
Setting Up Static Routes to Indirect Networks 4-4
Setting Up a Default Route 4-5
Configuring the NetBlazer as a Domain Name System Client 4-6
Testing the IP Router Configuration 4-6
What's Next 4-7

5 Dedicated IP Interface Configuration 5-1
Setting Up a Dedicated PPP Interface Link 5-1
Setting Up a Dynamic Backup for a Dedicated PPP Interface 5-2

6 Dynamic IP Interface Configuration 6-1
Setting Up a Single-Line Dynamic Interface 6-1
Setting Up Multiline Load Balanced Interfaces 6-4
General Guidelines 6-5
Using Ipdial to Set Up a Dynamic Interface 6-6
Setting Up Balanced Routes 6-11

7 Using Auto-Routes 7-1

8 Using Proxy ARP 8-1

9 IP Packet Filtering 9-1
Filtering Network IP Addresses 9-2
Using Filter Lookup to Check a Filter 9-3
Filtering Destination Port Numbers 9-3
Filtering Source and Destination Address Pairs 9-6
Deleting a Filter 9-7

10 Modem Server Configuration 10-1
Setting Up Dial-Out Destination Records 10-1
Adding a Dial-Out Destination 10-2
Using Chat to Automatically Log In to a Remote System 10-3
Using Characteristics Groups 10-3
Preconfiguring a Modem for a Dial-Out Destination 10-4
Restricting the Use of a Line for Specific Dial-Out Destinations 10-6
Setting Up a Modem Pool 10-7

Allowing Direct Number Dialing 10-8

11 User IDs and Destination Groups 11-1
First Decide Where to Keep the NetBlazer User Records 11-1
Adding Local User Records 11-2
Setting Up User Destination Groups 11-4
Automatically Connecting a User to a Specific Destination 11-7

12 Setting Up Callback Security 12-1
Setting Up a Callback Request Line 12-1
Callback with Auto-Telnet 12-1
Packet Mode Callback 12-2

13 Setting Up a Raw TCP Link 13-1
Configuring a Line for a Raw Connection 13-1
Assigning a Characteristic Group 13-1
Changing the Line's IP Address 13-2
Starting the Raw Server 13-2
Stopping a Raw Connection 13-2

14 Network Management 14-1
Booting the NetBlazer from a UNIX Host 14-1
Using Remote Configuration Files 14-4
Using Local and Remote Password Files 14-4
Loading a Remote Password File at Boot Time 14-5
Using a Remote Password File in Addition to the Local Passwd File 14-5
Getting Password Records from a Domain Name Server 14-5
Using Syslog to Monitor NetBlazer Activity 14-6
Sending Syslog Messages to a UNIX Host 14-6
Verifying that Syslog Messages Are Reaching the Host 14-7
SNMP Configuration 14-8
Default Settings 14-8
Community Groups and Security 14-8
The Telebit Enterprise MIB 14-9
SNMP Configuration Procedure 14-10

15 IPX Configuration 15-1
Verifying the Host Name 15-3
Host Name 15-3
Assigning an Internal Network Number and IPX Address 15-3
IPX Numbering and Addressing 15-3
Assigning an Internal Network Number 15-4
Assigning an IPX Address 15-5
Adding Interfaces and Assigning an IPX Address to Each Interface 15-5
Adding Interfaces 15-5
Assigning IPX Addresses to Interfaces 15-5
Specifying Packet Frames 15-6
Configuring the NetBlazer to Use IPX SAP 15-6

Listening for IPX SAP Information 15-6
Broadcasting IPX SAP Information 15-7
Configuring the NetBlazer to Use IPX RIP 15-8
Listening for IPX RIP Information 15-8
Broadcasting IPX RIP Information 15-8
Sending IPX Packets Through an IP Tunnel 15-9
Adding a Peer IP Address 15-9
Adding a Route for the IP Tunnel 15-9
Configuring a Dynamic IPX Interface 15-10
Setting Up a Dynamic Interface 15-10
Using Pppdial to Set Up a Dynamic Interface 15-11
Adding a Route for the Dynamic Interface 15-12
Viewing the Results 15-14
Saving the NetBlazer System Configuration 15-15
Configuring the Remote NetBlazer 15-15
IPX Pinging Between NetBlazers 15-15
Adding a SAP Table Entry 15-16
Keeping a Connection Open 15-16
Using the Remote Shell 15-17
Introduction 15-17
Before You Start 15-17
Installing the Remote Shell 15-18
Configuring the Remote Shell 15-18
Calling a NetBlazer with the Remote Shell 15-20
Using the WATCHPPP.EXE Program 15-21
Communicating with a File Server 15-21
Logging Off and Closing the Session 15-21
Using the Remote Shell Management Utilities 15-22
Using the Remote Shell Help 15-22

16 AppleTalk Configuration 16-1
Default Settings 16-1
General 16-2
Preplanning 16-2
The NetBlazer as an ARA Server 16-3
The NetBlazer as a Dial-Up Router 16-4
System Administration Considerations 16-5
Configuring the NetBlazer's Ethernet Port 16-5
Dynamic Link Setup 16-7
Asynchronous Dynamic Link 16-7
Synchronous Links 16-8
ARA Configuration 16-9
User Names and Passwords 16-9
Callback 16-10
Home Zone 16-10
Zone Filtering 16-11
Guest Access 16-11

ADSP Server 16-11
Maintenance Functions 16-12
ARA Users 16-12
Dynamic PPP Links 16-12

A NetBlazer File Definitions A-1
Editing a NetBlazer File Using MS-DOS A-3
STARTUP.CNF File Definition A-3
NetBlazer PASSWD File A-4
Editing a Copy of the UNIX Password File A-6
Loading a Password File into the NetBlazer A-8
MODEMCAP.TXT File Definition A-8
Command Line Formats A-8
Required Tag Commands A-10
Specific Function Tags A-14
Creating New Function Tags A-15
Using The Debug Modemcap Command A-15
Modem MIB Support Tags A-15
CHAT.TXT File Definition A-16
Chat Script Commands A-16
Chat Script Examples A-18
Telebit Enterprise MIB A-20

B Line Assignments B-1
Synchronous Lines B-1
Asynchronous Lines B-1

C AppleTalk C-Style Octal Table C-1

General Information

Introduction 1

This chapter provides a functional overview of the NetBlazer followed by a descriptions of the various roles that the NetBlazer plays in Transmission Control Protocol/Internet Protocol (TCP/IP), Internetwork Protocol Exchange (IPX), and AppleTalk environments

Functional Overview

The NetBlazer is a special-purpose system primarily designed to route data between serial lines and TCP/IP, IPX, and AppleTalk network segments. Physically, it consists of a CPU motherboard, a high-density diskette drive, a power supply, and several adapter boards. The adapter boards provide the physical connections to the interconnected Local Area Networks (LANs) and the serial lines.

The NetBlazer's proprietary operating system and control software provide the following functions:

- **Command Interpreter** – provides the user interface to the NetBlazer that allows the users to control the NetBlazer operation.
- **Disk Management** – includes a set of utilities used to manage the files on the NetBlazer's diskette.
- **User Authentication and Security** – prevent unauthorized access to the NetBlazer and its associated facilities.
- **TCP/IP Control and Services** – allow the NetBlazer to participate in a TCP/IP environment.
- **IPX Control and Services** – allow the NetBlazer to participate in an IPX environment.
- **AppleTalk Control and Services** – allow the NetBlazer to participate in an AppleTalk environment.
- **Serial Line Control** – regulates the interaction of the NetBlazer with devices attached to the NetBlazer's asynchronous and synchronous serial lines.
- **Network Management and Diagnostics** – provide the facilities used by a system administrator to oversee the operation of the NetBlazer on the network.

The NetBlazer is a multipurpose, multiprotocol device that serves a variety of functions in TCP/IP, IPX, and AppleTalk environments. You can use the NetBlazer as:

- A dial-up and leased line router for transferring IP, IPX, and AppleTalk packets over the Public Switched Telephone Network (PSTN)
- A terminal server that allows remote users access to the network
- A modem server that allows users on the network to gain access to outside services
- An AppleTalk Remote Access (ARA) server that allows remote Macintosh users to gain access to an AppleTalk server

Using the NetBlazer as a Router

The primary function of the NetBlazer is to act as a dial-up or leased line router to send IP, IPX, and AppleTalk packets between geographically distant networks over the public telephone network (see Figure 1-1).

As a dial-up router, the NetBlazer allows you build a wide area network without using expensive leased lines. You can configure the NetBlazer to set up multiple connections automatically across the telephone network, thus increasing the overall throughput of the link.

When ISDN terminal adapters or Switch 56 CSU/DSUs are connected to the synchronous ports, you can configure the NetBlazer to use the V.25*bis* dialing protocol to establish a dial-up connection over a switched digital network.

The NetBlazer can be set up as a leased line router with the unique ability to automatically establish a dial-up backup connection should the leased line connection fail.

Figure 1-2 shows the NetBlazer serving as a router that transfers packets through the telephone network between a remote workstation, personal computer (PC), or Macintosh on one end and a local network on the other. The remote system must be equipped with software that transmits packets over SLIP, PPP or ARA. For example, a PC with Telebit's Remote Shell sends IPX packets to the NetBlazer.

The NetBlazer also can serve as a gateway between Ethernet or Token Ring LANs, as shown in Figure 1-3.

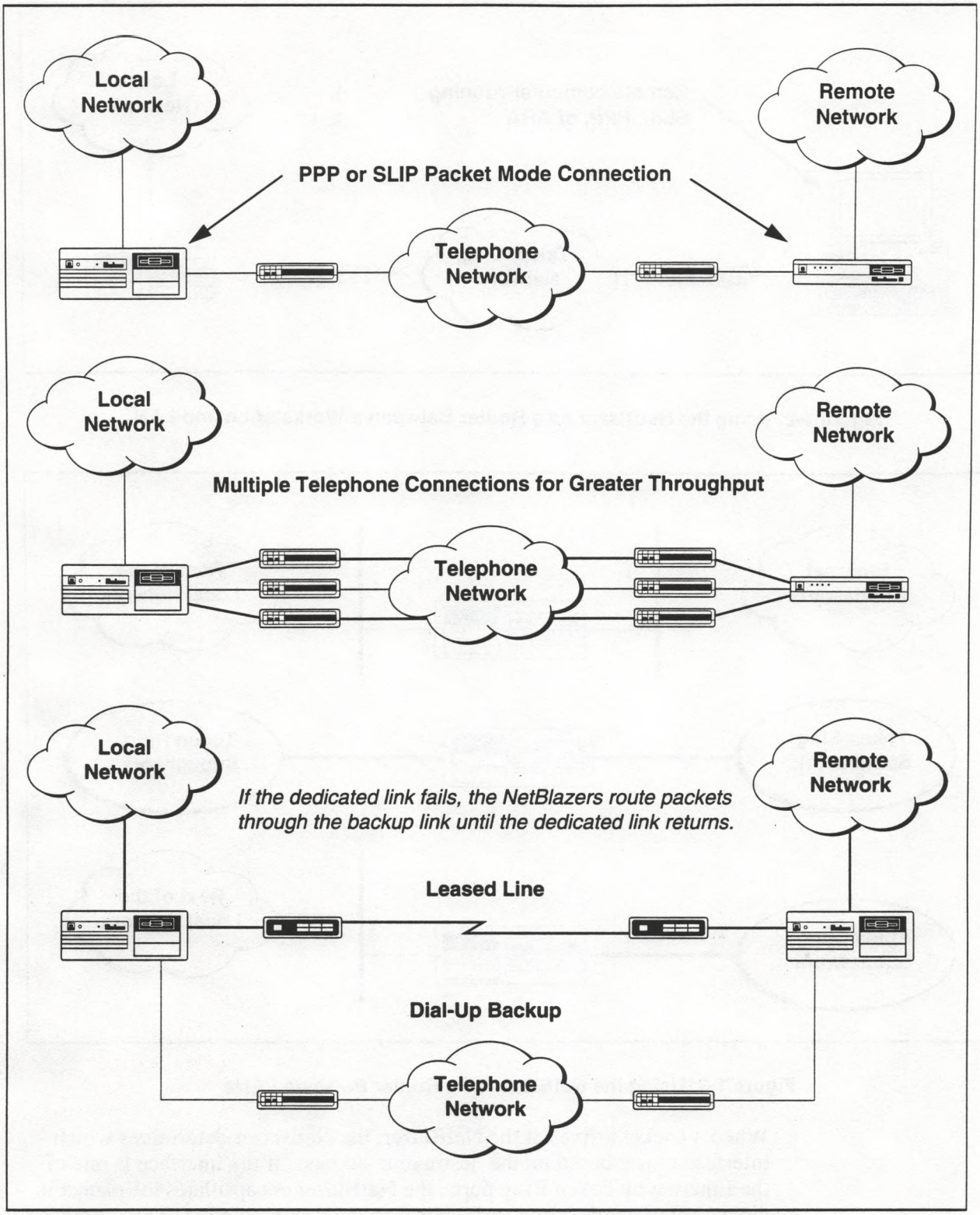


Figure 1-1. Using the NetBlazer as a Dial-Up and Leased Line Router

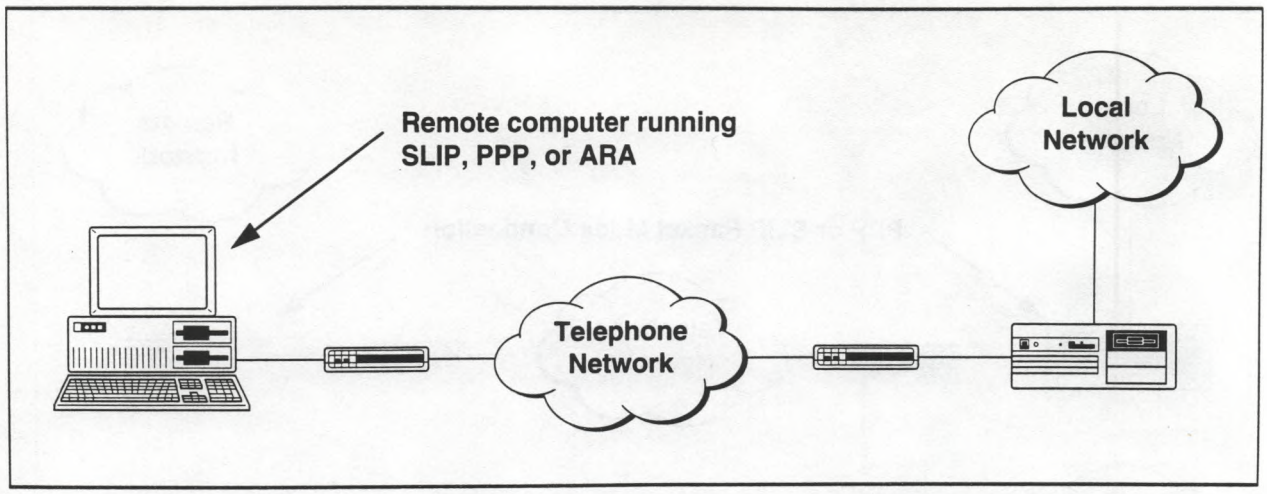


Figure 1-2. Using the NetBlazer as a Router Between a Workstation and LAN

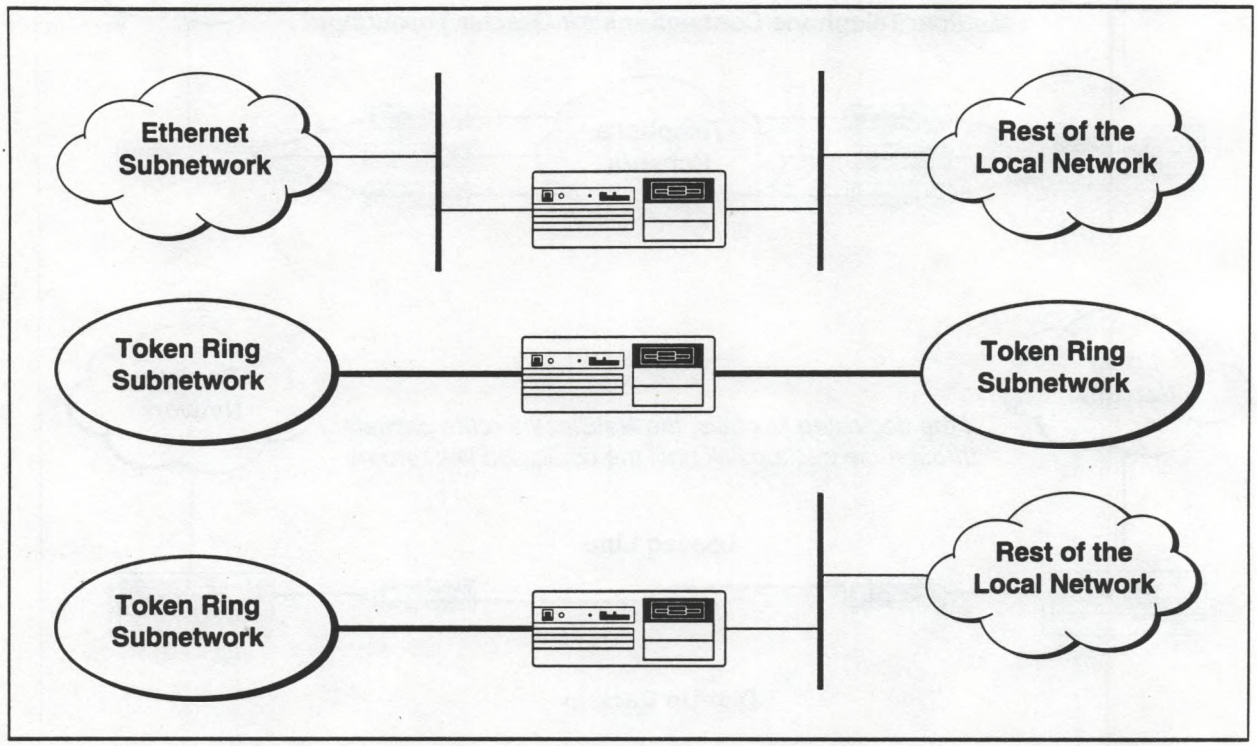


Figure 1-3. Using the NetBlazer as a Router Between LANs

When a packet arrives at the NetBlazer, the NetBlazer determines which interface to use based on the destination address. If the interface is one of the Ethernet or Token Ring ports, the NetBlazer encapsulates the packet in a physical network frame and sends it to the destination host or to another gateway on the network for further routing.

If the interface is a dynamic dial-out interface, the NetBlazer checks for an existing telephone link to the remote site. If a telephone link does not exist, the local NetBlazer gets the telephone number for the interface from its dial-out record and calls the remote NetBlazer.

When a modem connection is established, the answering NetBlazer starts a caller authentication process to verify that this is an authorized connection. If the calling NetBlazer responds with valid user ID, password, and crypto responses, the link is established.

When a link exists, the sending NetBlazer encapsulates packets in Serial Line Internet Protocol (SLIP) or Point-to-Point Protocol (PPP) frames and sends them to the receiving NetBlazer over the telephone network. The dynamic interface record tells the NetBlazer whether to use SLIP or PPP packet framing.

For additional information on setting up the NetBlazer interfaces to route packets between local and remote networks, refer to Chapter 2, NetBlazer Interface Descriptions.

For instructions on how to configure the NetBlazer as a TCP/IP, IPX, or AppleTalk router, refer to the following chapters:

- Chapter 4, IP Router Configuration
- Chapter 5, Dedicated IP Interface Configuration
- Chapter 6, Dynamic IP Interface Configuration
- Chapter 15, IPX Configuration
- Chapter 16, AppleTalk Configuration

Using the NetBlazer as a Terminal Server

As a terminal server, the NetBlazer allows remote users to gain access to the local IP and IPX network hosts and services.

The NetBlazer/ACS software option, which you can purchase separately, allows remote users to dial in to the NetBlazer and access the IPX network services as a remote NetWare node.

Remote IP users can a use an asynchronous terminal (or computer with communications software) to dial in to the NetBlazer and start a telnet session with a local IP host. Upon receiving a call, the NetBlazer prompts the caller for a login ID and password. Every user who logs in to the NetBlazer must have an assigned user record. If the caller responds with a valid user ID and password, he or she is connected to the NetBlazer in command mode. The user can then enter a command to start a telnet session with a TCP/IP host on the network.

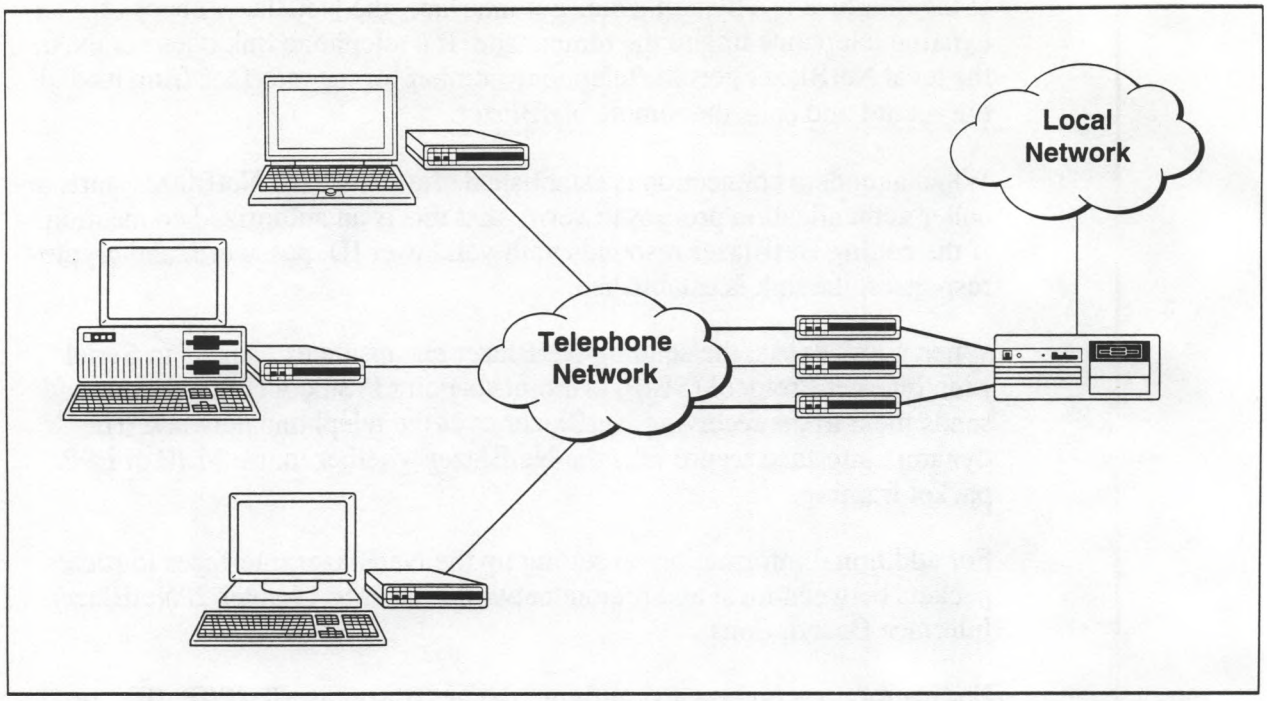


Figure 1-4. Using the NetBlazer as a Terminal Server

Instructions for setting up user accounts are provided in Chapter 11, User IDs and Destination Groups.

The NetBlazer can be configured to bypass the login process and start a telnet session with a designated host by assigning a telnet command to an asynchronous line. Then whenever a call is received on that line, the caller is connected automatically with the specified host as if he or she had called the host directly.

An alternative way to automatically connect a caller to a host is to assign a login command to the user that starts a telnet or rlogin session with a specified host when the user logs in to the NetBlazer. The advantage of this method is that it does not require dedicating an asynchronous line to a single host.

Using the NetBlazer as a Modem Server

As a modem server, the NetBlazer allows TCP/IP, IPX, and AppleTalk network users to access outside services through the modems connected to the NetBlazer (see Figure 1-5).

To establish a dial-out connection from the NetBlazer, TCP/IP network users must first log in to the NetBlazer through a telnet session, and then issue a command to call the remote site. You also can set up the NetBlazer to allow users to telnet to a modem and call out using the modems dial command.

Refer to Chapter 10, Modem Server Configuration, for instructions on how to configure the NetBlazer as a modem server on an TCP/IP network.

The NetBlazer/ACS software option, which you can purchase separately, is required to access the NetBlazer's modem pool over an IPX network.

AppleTalk users can use a network terminal communications package, such as MacTerminal or PacerTerm, to log in to the NetBlazer and then issue a NetBlazer command to call out to a remote site.

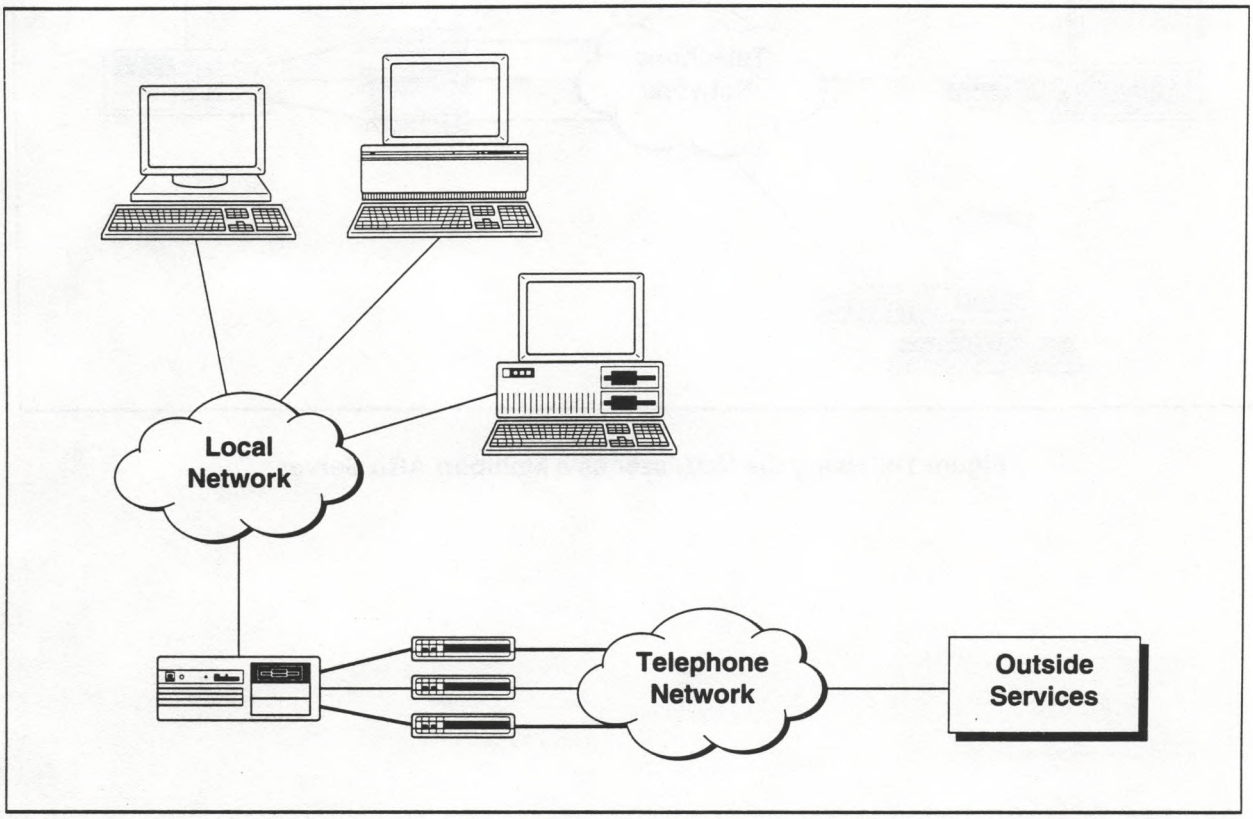


Figure 1-5. Using the NetBlazer as a Modem Server

Using the NetBlazer as an ARA Server

Figure 1-6 shows the NetBlazer serving as an multiport ARA server. Any Macintosh using ARA software can access the servers on an AppleTalk network through a dial-in ARA connection to the NetBlazer.

Instructions for configuring the NetBlazer as an ARA server are provided in Chapter 16, AppleTalk Configuration.

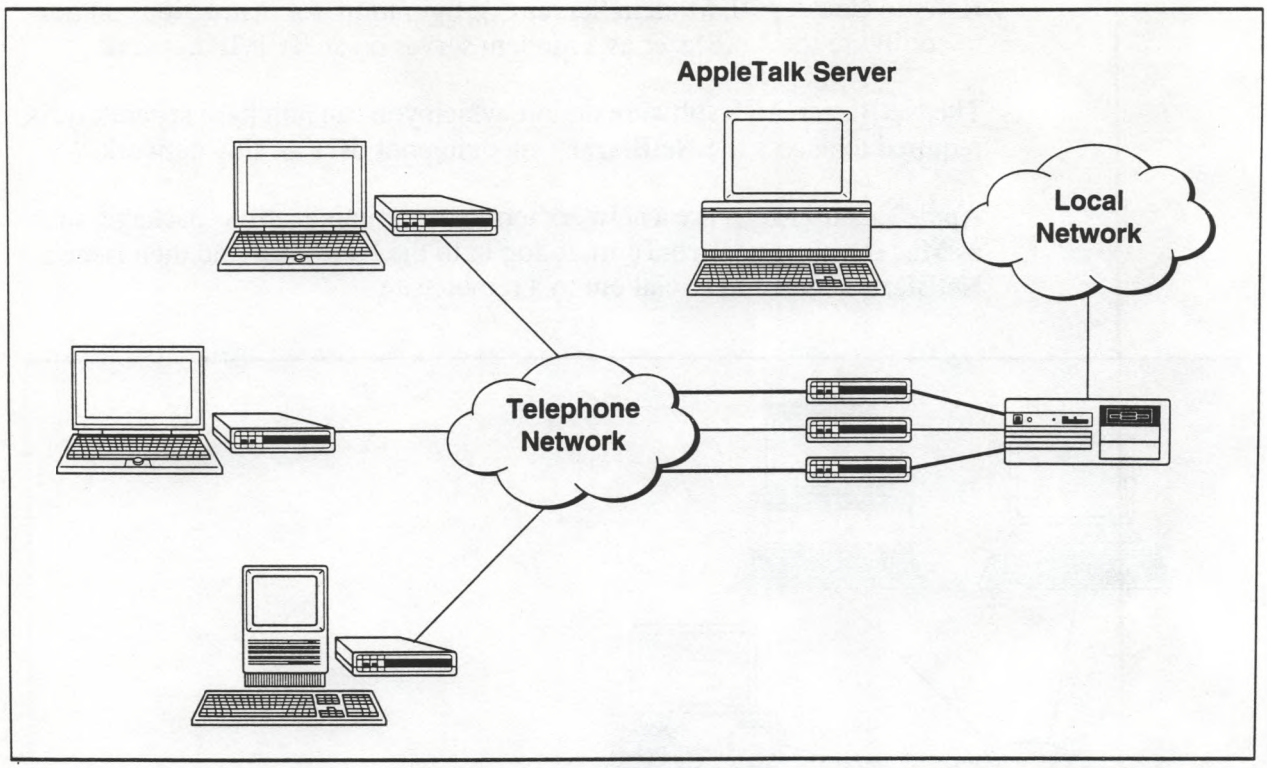


Figure 1-6. Using the NetBlazer as a Multiport ARA Server

NetBlazer Interface Descriptions 2

The NetBlazer uses three types of interfaces: LAN, dynamic, and dedicated serial line interfaces.

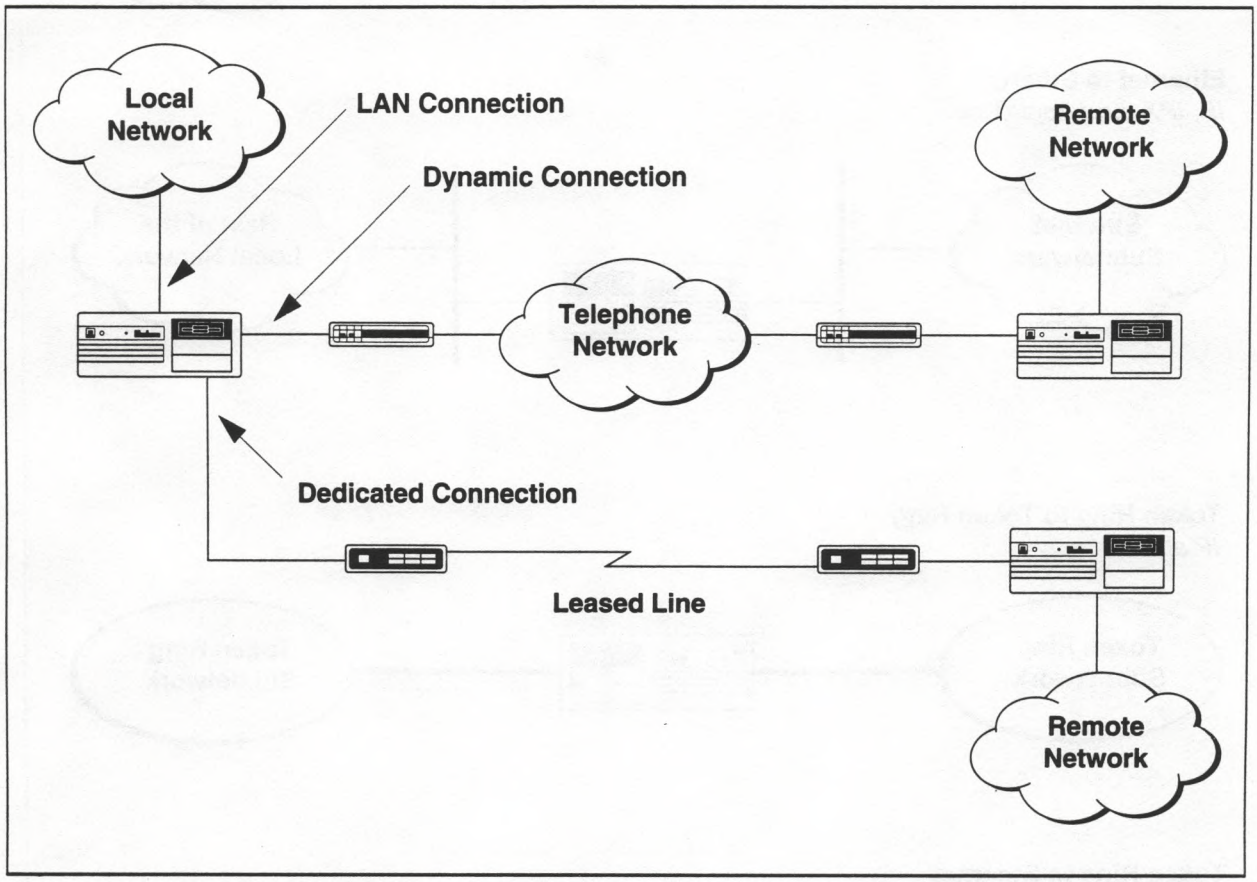


Figure 2-1. NetBlazer Interface Connections

LAN interfaces are automatically created for each Ethernet and Token Ring board installed in the NetBlazer.

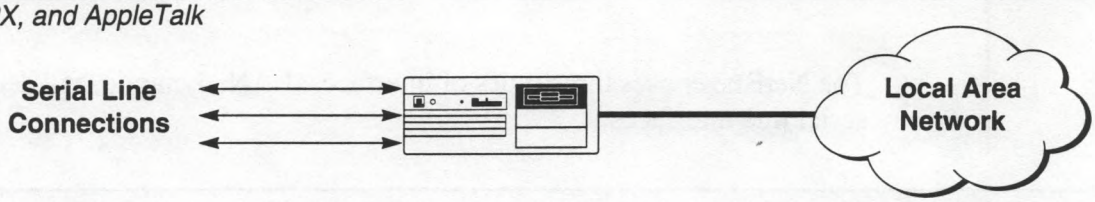
Dynamic interfaces provide dial-up PPP or SLIP links to route packets over the public switched telephone network.

Dedicated interfaces use PPP or SLIP packet framing to route packets over dedicated point-to-point synchronous or asynchronous serial lines.

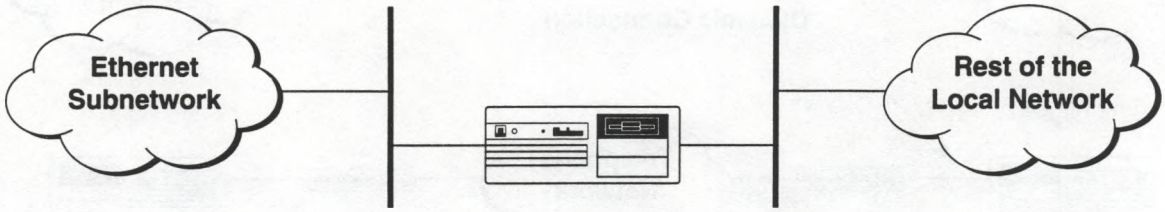
LAN Interfaces

Figure 2-2 shows four common ways that the NetBlazer is used to route IP, IPX, or AppleTalk packets between LANs.

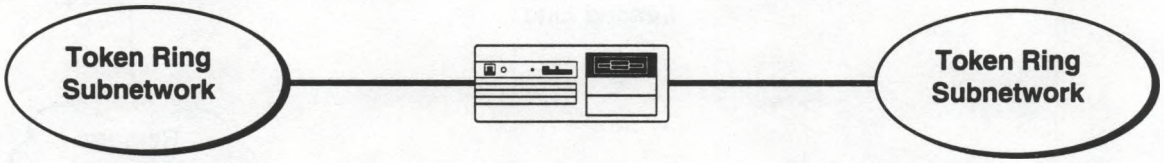
Serial Line to LAN
IP, IPX, and AppleTalk



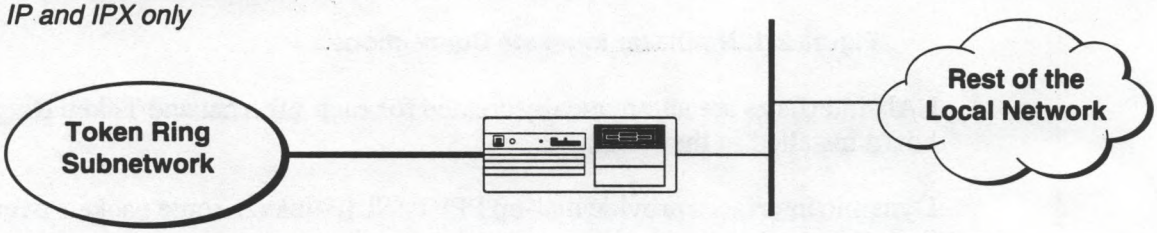
Ethernet to Ethernet
IP, IPX, and AppleTalk



Token Ring to Token Ring
IP and IPX only



Token Ring to Ethernet
IP and IPX only



Note: *The NetBlazer does not support routing AppleTalk packets through a Token Ring port.*

Figure 2-2. LAN Interface Configurations

Routing IP Packets Through a LAN Interface

To configure the NetBlazer as an IP router:

- Assign a global IP address to the NetBlazer.
- Assign an IP address to each Ethernet and/or Token Ring interface that is used to route IP packets.
- Add a static route to the NetBlazer's IP routing table for each subnet that is directly accessible through the NetBlazer's LAN interface(s).
- Add IP routes to other LANs, which are not directly accessible to the NetBlazer. You have two choices: manually add static routes to the NetBlazer's routing table, or configure the NetBlazer to learn the routes to other indirect networks using RIP (Routing Information Protocol).
- If your network includes one or more domain name servers (DNS), configure the NetBlazer as a DNS client. This allows NetBlazer users to use domain names in place of IP addresses.

For instructions on how to configure the NetBlazer as an IP router, refer to Chapter 4, IP Router Configuration.

Routing IPX Packets Through a LAN Interface

To configure the NetBlazer as an IPX router:

- Assign the NetBlazer an internal network number and an IPX address.
- Add each LAN (Ethernet or Token Ring) interface to the IPX interface list.
- Assign an IPX address to each IPX interface.
- Add IPX routes to other LANs, which are not directly accessible to the NetBlazer. You have two choices: manually add static routes to the NetBlazer's routing table, or configure the NetBlazer to learn the routes to other indirect networks or services using IPX Routing Information Protocol (RIP) and IPX Service Advertising Protocol (SAP).

For instructions on how to configure the NetBlazer as an IPX router, refer to Chapter 15, IPX Configuration.

Routing AppleTalk Packets Through a LAN Interface

To configure the NetBlazer as an AppleTalk router:

- Determine whether the NetBlazer is going to function as a node on the network (ARA server), or as a router. If it is to function as a router, decide if it will be a seed or nonseed router. Nonseed routers automatically learn routes, while seed router maintain a static list of routes.
- Add the Ethernet LAN interface to the AppleTalk interface list. If you have selected seed, add the network number(s) and zones for each Ethernet LAN interface.

For instructions on how to configure the NetBlazer as an AppleTalk router, refer to Chapter 16, AppleTalk Configuration.

Dedicated Serial Line Interfaces

Figure 2-3 shows four common ways that the NetBlazer uses dedicated interfaces to route packets over synchronous or asynchronous point-to-point links.

Setting Up a Dedicated Interface Link

To set up a dedicated interface connection between two NetBlazers or between a NetBlazer and a workstation running PPP or SLIP:

- Enter an **interface attach** <line-name> slip|ppp <interface> command. This designates the specified line as a PPP or SLIP interface, which is used to route packets to the other end of a point-to-point link.

  PPP framing is required in most cases. SLIP framing may be used only for an asynchronous IP link that does not require a dial-up backup link.
- If the interface is used for IP packet routing, add an IP route for each IP subnet on the opposite side of the link to the IP routing table.
- If the interface is used to route IPX packets, add the interface to the IPX list of interfaces, and add an IPX route for each IPX subnet on the opposite side of the link to the IPX routing table.
- If the interface is used to route AppleTalk packets, add the interface to the AppleTalk list of interfaces and issue the **appletalk route learn** command to learn the zones within the network to which each NetBlazer is connected.
- Repeat the above procedure on the opposite side of the link.

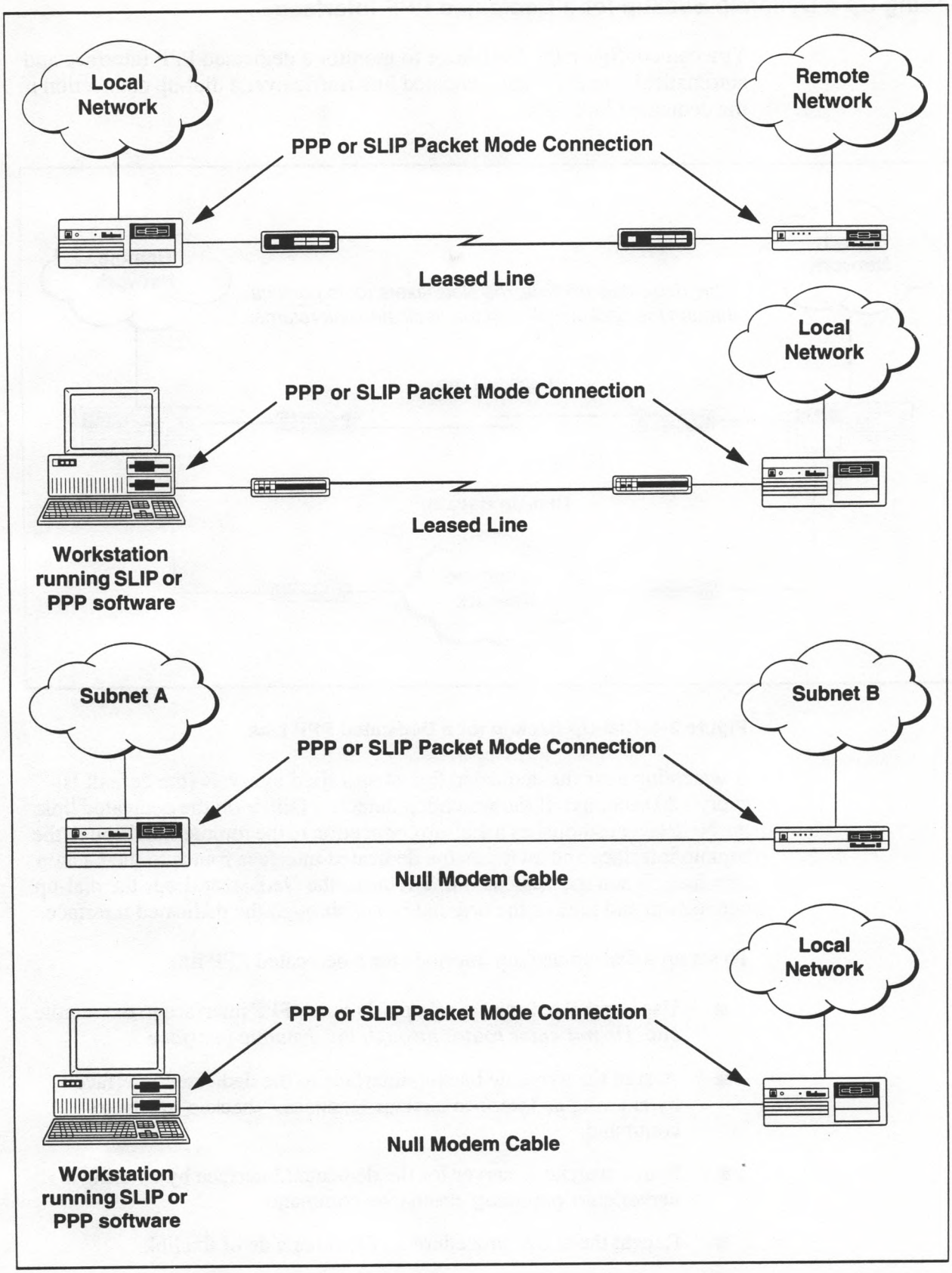


Figure 2-3. Dedicated Interface Configurations

Setting Up a Dynamic Backup for a Dedicated PPP Interface

You can configure the NetBlazer to monitor a dedicated PPP interface and automatically redirect the dedicated link traffic over a dial-up connection if the dedicated link fails.

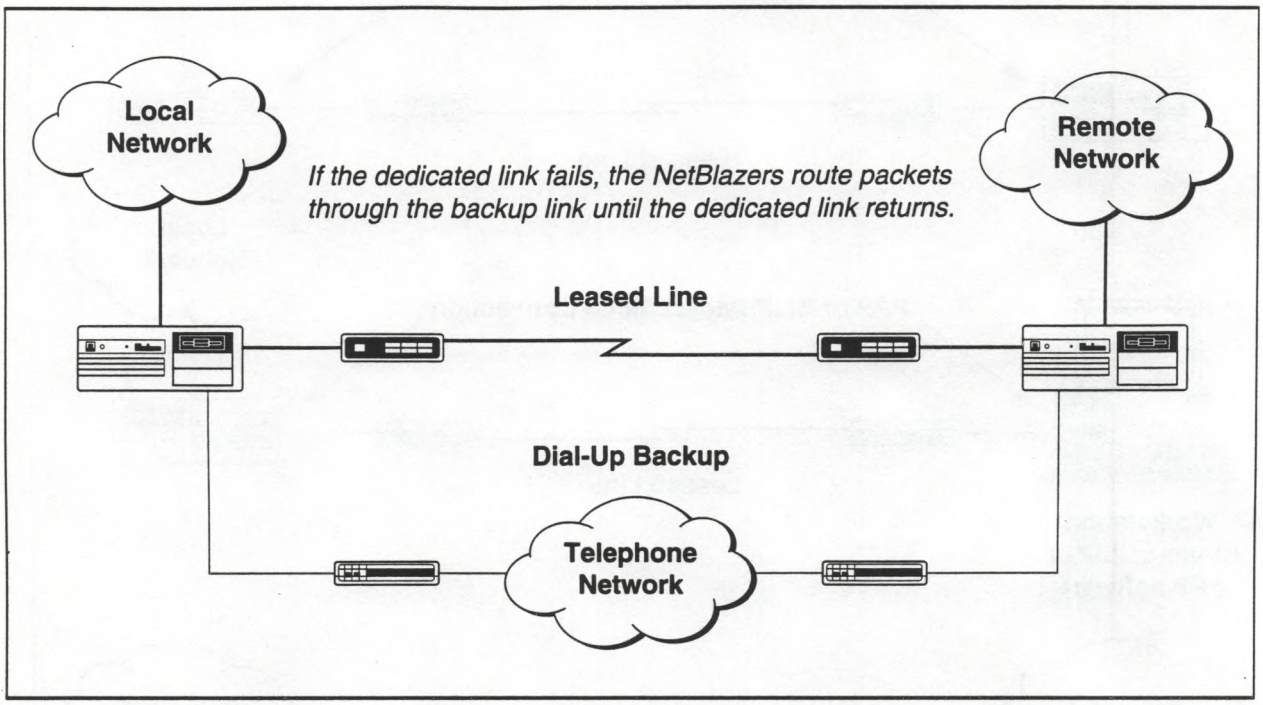


Figure 2-4. Dial-Up Backup for a Dedicated PPP Link

A watchdog tests the dedicated link at specified intervals (the default is every 120 seconds). If the watchdog detects a failure on the dedicated link, the NetBlazer establishes a dial-up connection to the remote site through the backup interface and switches the dedicated interface routes to the backup interface. When the dedicated link returns, the NetBlazer drops the dial-up connection and returns the original routes through the dedicated interface.

To set up a dial-up backup interface for a dedicated PPP link:

- Use **pppdial** or **ipdial** to set up a dynamic PPP interface to the remote site. *Do **not** enter routes through the dynamic interface.*
- Assign the dynamic backup interface to the dedicated interface by entering an **interface backup** <interface> <backup_interface> command.
- Start a watchdog server for the dedicated interface by entering a **server start watchdog** <interface> command.
- Repeat the above procedure on the other side of the link.

Figure 2-5 shows three common ways that the NetBlazer uses dynamic interfaces to route packets between local and remote LANs through the public telephone network.

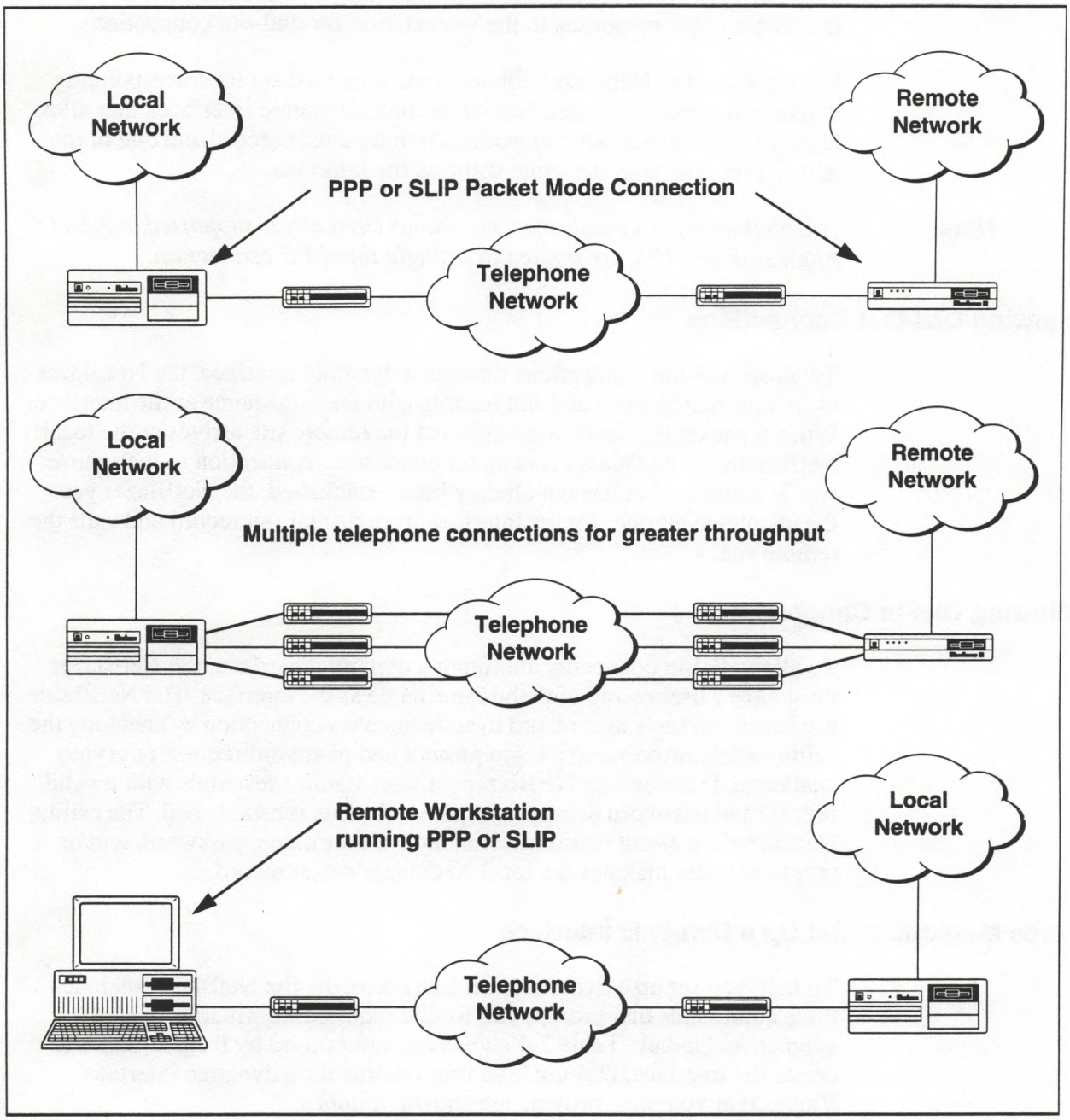


Figure 2-5. Dynamic Interface Configurations

You can set up one or more dynamic links between two NetBlazers, or you can set up a single dial-up connection between a remote workstation and the local NetBlazer.

If you are setting up a dynamic interface between a NetBlazer and a remote workstation, the workstation must use a PPP or SLIP software package that can be configured to respond correctly to the NetBlazer's login sequence. You also may need to set up a custom chat script on the NetBlazer to provide the proper login responses to the workstation for dial-out connections.

For NetBlazer to NetBlazer connections, you must set up corresponding dynamic interfaces on each side of the link. Dynamic interfaces that allow both dial-in and dial-out connections require a user record and one or more dial-out records with the same name as the interface.

Note: *Load balancing over multiple connections currently is supported only by IP. AppleTalk and IPX are limited to a single line PPP connection.*

Allowing Dial-Out Connections

To allow dial-out connections through a dynamic interface, the NetBlazer must have one or more dial-out records with the same name as the interface. When a packet that has a destination at the remote site arrives at the local NetBlazer, the NetBlazer checks for an existing connection to the remote site. If a connection has not already been established, the NetBlazer gets the telephone number for the interface from its dial-out record and calls the remote site.

Allowing Dial-In Connections

To allow dial-in connections through a dynamic interface, the NetBlazer must have a user record with the same name as the interface. The NetBlazer uses the interface's user record to authenticate a connection by checking the calling site's response to a login prompt and password request or crypto challenge. If the calling NetBlazer (or workstation) responds with a valid user ID and password or crypto response, the link is established. The calling NetBlazer's dial-out record must include a user name, password, and/or crypto key that matches the local NetBlazer's user record.

Three Methods to Set Up a Dynamic Interface

To help you set up a dynamic interface correctly, the NetBlazer includes three commands that prompt you for the required information: **pppdial**, **slipdial**, and **ipdial** . Table 2-1 shows the values used by these routines to create the interface, dial-out, and user records for a dynamic interface. Values that you must provide are shown in *italics*.

Table 2-1. Dynamic Interface Values

Fields	Pppdial Values	Slipdial Values	Ipdial Values
Interface Record			
interface name	*remote hostname*	*remote hostname*	*user defined*
framing	ppp	slip	*slip or ppp*
MTU/MRU	1500	1006	*user defined*
queue max	8 packets	8 packets	8 packets
VJ header compression	auto	auto	auto
packet mode timeout	180 seconds	180 seconds	180 seconds
Dialout Record			
dialout name	interface name	interface name	interface name
phone number	*user defined*	*user defined*	*user defined*
characteristics group	dialout	dialout	*user defined*
user name	local hostname	local hostname	*user defined (note 2)*
password	*user defined (note 1)*	*user defined (note 1)*	*user defined (note 2)*
crypto key	*user defined (note 1)*	*user defined (note 1)*	*user defined (note 2)*
chat script	ics	ics	*user defined*
character mode timeout	60 minutes	60 minutes	60 minutes
User Record			
user name	interface name	interface name	interface name
password	*user defined (note 1)*	*user defined (note 1)*	*user defined*
crypto key	*user defined (note 1)*	*user defined (note 1)*	*user defined*

Notes:

1. The **pppdial** and **slipdial** routines use the same password or crypto key to authenticate both inbound and outbound connections.
2. The dial-out record user name, password, and crypto key must match the user record values on the remote system.
3. Any line used for a dynamic interface connection must not be set to use XON/XOFF flow control. Refer to the **line** command description in the *NetBlazer Command Reference Manual.*

The **pppdial** and **slipdial** routines are the easiest to use because they only require a minimum amount of information and use the NetBlazer's default values whenever possible. These two routines are best for setting up a single line PPP or SLIP connection between two NetBlazers.

The **ipdial** routine is a more complex and flexible routine that gives you more control over setting up a dynamic interface. This routine is best for creating multiple interfaces used to distribute IP traffic over several dial-up connections between two sites.

Choosing PPP or SLIP Framing

When choosing between PPP and SLIP framing, remember that both sites must agree on the framing used. If any of the following conditions apply to your application, use PPP framing:

- The interface is used for a synchronous dynamic connection.
- The interface is used for AppleTalk or IPX packet routing.
- The interface is used with a remote workstation application that uses a PPP feature such as dynamic address assignment.
- The interface is used as a dial-up backup for a dedicated link.

If none of these conditions applies to your application, use SLIP framing for a faster connection.

Routing Packets Through a Dynamic Interface

After setting up a dynamic interface, you must configure the NetBlazer to route packets through that interface. If the interface uses PPP framing, you can route IP, IPX, or Appletalk packets to a remote site through the same interface. Do not set up separate interfaces to the same site for each protocol.

IP Packet Routing

To route IP packets over a dynamic connection, the NetBlazer requires an IP route for each subnet on the opposite side of the link.

If you configure the dynamic interface to allow dial-out connections, you must add one or more static routes for the remote site to the NetBlazer's IP routing table.

If you configure the dynamic interface to only allow dial-in connections, you have two options. You can use static routes, or you can configure the dynamic interface to automatically add its routes to the routing table when a connection is established from the remote site.

Auto-routes differ from static routes in that they are only available while a dynamic connection is established and are removed from the routing table when the connection is dropped.

Refer to Chapter 6, Dynamic IP Interface Configuration, for instructions on how to set up dynamic interfaces to route IP packets to a remote site. An example of how to set up auto-routes for a remote site is provided in Chapter 7, Using Auto-Routes.

IPX Packet Routing

To route IPX packets through a dynamic interface, you must add the interface to the IPX interface list and set up an IPX route for each subnet located at the remote site.

Refer to Chapter 15, IPX Configuration, for instructions on how to set up a dynamic interface to route IPX packets to a remote site.

AppleTalk Packet Routing

To route AppleTalk packets through a dynamic interface, you must add the interface to the AppleTalk interface list, and then enter static routes, or use the **appletalk route learn** command to learn the zones within the network to which the NetBlazer is connected.

Refer to Chapter 16, AppleTalk Configuration, for instructions on how to set up a dynamic interface to route AppleTalk packets to a remote site.

Setting Up a Synchronous Dynamic Interface

The procedure to set up a dynamic interface that uses a synchronous line is the same as setting up a dynamic interface for an asynchronous line with the following additional requirements:

- Make sure that the synchronous line is connected to a terminal adapter or DSU/CSU that supports the V.25bis protocol.
- Enable the V.25bis protocol on the synchronous line by issuing a **line v25bis** <line-name> **on** command.
- Assign the v25dialout characteristics group to the line by issuing a **line characteristics** <line-name> **v25dialout** command.
- Use **ipdial** to create a dynamic interface for the synchronous link. When you are prompted for the dial-out record's line characteristics, enter **v25dialout**.
- Repeat this procedure on the remote NetBlazer.

Getting Started 3

This chapter covers the basic steps the system administrator must perform in preparing the NetBlazer for configuration of the IP, IPX, and AppleTalk protocols. Step-by-step procedures to establish basic communications with the NetBlazer in order to perform the configuration of your desired protocols and NetBlazer functions are provided.

Overview

This section assumes you have completed the NetBlazer hardware installation as described in the *NetBlazer Installation Guide*. All desired option boards and electrical connections to the NetBlazer must have been installed before you can proceed.

Customizing The STARTUP.CNF File

Configuration information about the protocol(s) routes, users, and any special functions you wish to use is saved in the NetBlazer's STARTUP.CNF file. This file is used upon start-up or rebooting to automatically configure the NetBlazer for use in your network environment.

However, before the NetBlazer can function on your network, the STARTUP.CNF file must contain a few important items of information about the NetBlazer's identity. You must supply this information using one of two basic methods to edit the STARTUP.CNF file:

- Issuing commands to the NetBlazer to perform the desired configuration (on-line editing);
- Manually editing the NetBlazer's STARTUP.CNF file on a DOS computer (off-line editing).

Issuing commands to the NetBlazer to perform configuration occurs by communicating directly with the NetBlazer. This method is based on techniques of accessing the NetBlazer that do not require it having a network identity. Logging into the NetBlazer directly may be accomplished through four methods, depending on the protocol used on the network to which your NetBlazer is attached.

Manually editing the NetBlazer's STARTUP.CNF file (to preconfigure the NetBlazer so that it can be reached from your network) requires the use of a PC running DOS to edit the file. Once this is done and NetBlazer is booted with the edited file on the system diskette, you can then log into the NetBlazer through a telnet (IP protocol only) session from a host on the network.

Communications with the NetBlazer can be established using the following four methods:

- **Over an IPX network** – Use a PC running Windows 3.1 and the Telebit NetBlazer Configuration Utility on an IPX network to which the NetBlazer is attached. A color monitor and a mouse are recommended. Contact your Telebit representative for further information about the NetBlazer Configuration Utility.
- **Over an AppleTalk network** – Use a Macintosh containing an Ethernet board running a communications program that supports the Apple Communications Toolbox (i.e., MacTerminal 3.0, or PacerTerm) that is connected to the same network Ethernet segment as the NetBlazer.
- **Direct asynchronous connection (all protocols)** – Use a terminal (or computer running terminal emulation software) connected to one of the NetBlazer's asynchronous ports.
- **Telnet over an IP network** – If setting up an administrative workstation is not feasible and you need to access the NetBlazer from a TCP/IP workstation, you can preconfigure the NetBlazer system diskette by using a text editor on an MS-DOS system to edit the STARTUP.CNF file, and then telnet to the NetBlazer from a host on the Ethernet segment attached to the NetBlazer's en0 interface to complete the configuration.

In the case of a direct asynchronous connection, you must have a dial-in workstation that you can use to call in to the NetBlazer, or an asynchronous terminal connected to the NetBlazer through a null modem cable. Refer to your *NetBlazer Installation Guide* for instructions on setting up an administrative workstation.

Off-line Editing the STARTUP.CNF File

In the event you configure the NetBlazer remotely by using the IP telnet function from a host on the Ethernet segment attached to the NetBlazer's en0 interface, it is necessary to preconfigure the NetBlazer system diskette by using a text editor on an MS-DOS system to edit the STARTUP.CNF file. See Using MS-DOS to Preconfigure the STARTUP.CNF File for instructions.

Note: *Because the STARTUP.CNF file contains a list of commands that are executed in sequence starting at the top of the file and working down, configuration commands that define parameters used by other commands must appear in the proper order. Several other considerations are also necessary in editing this file. For this reason, Telebit recommends off-line editing of the STARTUP.CNF file be limited to the basic procedure described in this chapter.*

On-line Editing Steps

Assuming you use the on-line method of editing the STARTUP.CNF file through a direct connection to the NetBlazer, the basic steps to get started (regardless of which protocol(s) you will be configuring) are:

Log In

The first step in configuration is to establish direct communications by logging in to the NetBlazer from your terminal or computer as "root".

Make Your Backup

You should make a backup copy of the distribution diskettes before you begin working with the NetBlazer. The NetBlazer provides a diskette copy command for this purpose. Use the copy as your working diskette.

Name Your NetBlazer

Once you have logged on to the NetBlazer, you will want to assign a host name to the NetBlazer. This name will appear as part of the command prompt.

Set the Clock

Set the time and date.

Change the Supervisor Password root account

Assign your new password to "root" to secure access to the NetBlazer.

Try Your New Root Password

Verify that you can log in to the NetBlazer using your new password by logging out, then back in. If it doesn't work, reboot the NetBlazer and repeat the above procedure.

Save Your Work

Issue the **save** command to record your changes in the STARTUP.CNF file.

The remaining portion of this chapter provides detailed procedures for performing the basic getting started steps.

Using MS-DOS to Back Up the System Diskette

Although the NetBlazer has its own operating system and disk utilities, its diskette file format is compatible with MS-DOS. Therefore as an alternative to using the NetBlazer's **diskcopy** command, you can use the **DISKCOPY** utility on an MS-DOS system that supports 3.5 inch high-density diskettes to make a backup copy of the system diskette. Refer to your MS-DOS Reference Manual for instructions on copying a diskette.

Note: *Because the NetBlazer uses a special boot block and loader, formatting a diskette on a PC and then copying the files over* ***will not*** *work. You must use DISKCOPY or its equivalent.*

Use the duplicate diskette as a working copy and put the original NetBlazer system diskette away in a safe place.

Using MS-DOS to Preconfigure the STARTUP.CNF File

Note: *If you have a terminal attached to one of the NetBlazer's asynchronous ports or a dial-in workstation that you can use to call into the NetBlazer, you do not need to preconfigure your STARTUP.CNF file. Skip ahead to Starting the NetBlazer and Logging in as Root on page 3-6.*

If you do not have a way to connect to the NetBlazer through one of the asynchronous ports, you can use an MS-DOS editor to preconfigure the STARTUP.CNF file so that the NetBlazer can be accessed from a TCP/IP workstation after it is powered up.

Using the MS-DOS **COPY** utility, copy DEFAULT.CNF to STARTUP.CNF.

Caution: *When editing the STARTUP.CNF file, use a text editor (such as edlin) or word processor that does not truncate or break lines that wrap around, and be sure to save the file in ASCII text format.*

If you have an IPX network, use the Telebit NetBlazer Configuration Utility on an IPX network to which the NetBlazer is attached. (Contact your Telebit representative for further information about the NetBlazer Configuration Utility.)

Edit the STARTUP.CNF file to include an **ip address** and **route** command as shown in **bold** below.

```
configure setconsole asy00
configure hostname NetBlazer
configure ip address 143.191.11.5
configure ip route add 143.191.11/24 en0
configure group add dialout
configure group add dialout
configure group modify dialout add dialout
configure group add v32dialout
configure group modify v32dialout add dialout
configure group modify v32dialout add v32
configure group add request
configure group modify request add request
configure group add pepdialout
configure group modify pepdialout add dialout
configure group modify pepdialout add pep
configure group add raw
configure group modify raw add raw
configure group add raw_dial
configure group modify raw_dial add raw
configure group modify raw_dial add dialout
configure group add v25dialout
configure group modify v25dialout add v25bis
configure ip route addprivate 127.0.0.1 loopback
configure server start telnet
configure server start ftp
configure server start rip
```

Notes:

1. *The addresses shown in this and other examples throughout this manual are for illustrative purposes only. You should choose an unused address from the address space of the LAN segment connected to the en0 interface.*
2. *If your NetBlazer is connected to a Token Ring network instead of an Ethernet network, use tr0 in place of en0 in the above example.*

These two commands provide the minimum information required to access the NetBlazer from a TCP/IP LAN workstation on the Ethernet segment attached to the NetBlazer's en0 interface.

The **ip address** command assigns a global IP address to the NetBlazer, and the **route add** command creates a route to the subnetwork that is attached to the NetBlazer through the en0 interface.

The **/24** in the **route add** command's IP address indicates that the route is for a subnetwork with the first 24 bits being the network portion of the address. This is equivalent to a subnet mask of 255.255.255.0.

You should now be able to power up the NetBlazer using the modified STARTUP.CNF file, and log in to the NetBlazer through a telnet session from any host that is on the Ethernet segment attached to the NetBlazer through the en0 interface.

On an AppleTalk Network

This method requires a Macintosh computer with an Ethernet connection to the network to which the NetBlazer is attached. If you do not have System 7 installed, you will need to have the Communications Toolbox with System 6. You will also need:

- A communications package, such as MacTerminal 3.0 (or later), PacerTerm, or any communications package that supports the Apple Communications Toolbox.
- The AppleTalk ADSP tool and a terminal tool (such as TTY tool or VT102 tool) installed in the Extensions folder in the System folder under System 7, or in the Communications folder in the System folder under System 6. These tools are supplied with MacTerminal 3.0 (or later), PacerTerm, or may be obtained from Apple's "Macintosh Communications Tools Basic Connectivity Set".

Procedure

1. Typically, these communications programs default to the serial communications port when first started. If this is true in your case, it is necessary to change the **Connection** setting under the **Settings** pull-down menu in the Communications Toolbox (see Figure 3-1).

   Select the ADSP Connection Tool in the Method: box, and ADSP in the Connection Type: box. You may also need to select the appropriate zone if there are more than one (a list of ADSP servers appears on the right side of the screen. An unconfigured NetBlazer will appear on the list as simply "NetBlazer"). Once you have made the appropriate selections, click on OK.

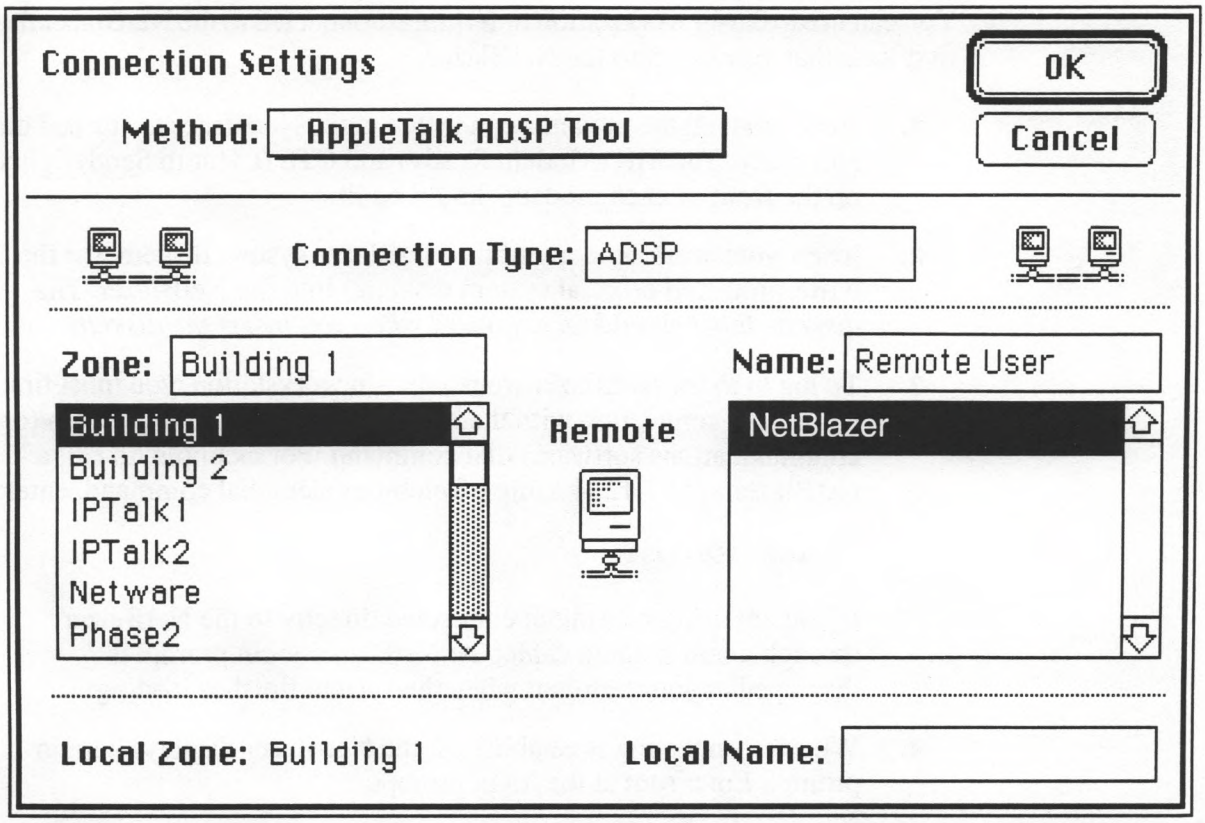


Figure 3-1. Communications Toolbox Screen

2. Initiate the connection to the NetBlazer. In the case of MacTerminal 3.0, select the Open Connection item under the **Session** pull-down menu (or press the Apple Command key and the I key together). Note that other communications packages use a different command.

3. The NetBlazer login prompt should then appear. This indicates that the NetBlazer is ready and waiting for you to enter your user ID:

```
Telebit's NetBlazer Version 2.0

NetBlazer login: root

NetBlazer: Top>
```

The NetBlazer commands are arranged in a tree-structured hierarchy, starting at the Top command level, and working down through several subcommand levels. Instructions for moving around and using the various commands are provided in the *NetBlazer Command Reference Manual*.

4. Proceed to the section *Using NetBlazer's Diskcopy to Back up the System Diskette*.

Using an Administrator's Workstation

You can use a dial-in workstation or terminal connected to the NetBlazer the first time that you log in to the NetBlazer.

1. Verify that all the modems connected to the NetBlazer are turned on and ready. The MR (Modem Ready) and CTS (Clear to Send) lights on the front of each modem should be lit.

2. Insert your working copy of the NetBlazer system diskette (or the write-protected original system diskette) into the NetBlazer. *The diskette label should face upward when you insert the diskette.*

3. To log in to the NetBlazer from a dial-in workstation, you must first establish a connection with the NetBlazer by using your modem (or communications software) dial command. For example, to call a NetBlazer at 555-1234 using a Telebit modem dial command, enter:

   ```
   atdt 555-1234
   ```

   If you are using a terminal connected directly to the NetBlazer through a null modem cable, the NetBlazer login prompt is displayed at your terminal when the system finishes loading.

4. When a connection is established, the NetBlazer displays a login prompt. Enter **root** at the login prompt.

```
Telebit's NetBlazer Version 2.0

NetBlazer login: root

NetBlazer:Top>
```

The NetBlazer then displays its command prompt. This indicates that the NetBlazer is ready and waiting for you to enter a command.

The NetBlazer commands are arranged in a tree-structured hierarchy, starting at the Top command level, and working down through several subcommand levels. Instructions for moving around and using the various commands are provided in the *NetBlazer Command Reference Manual.*

Using NetBlazer's Diskcopy to Back Up the System Diskette

If you have already made a backup copy of your NetBlazer system diskette on an MS-DOS system, skip ahead to the next section, Assigning a Host Name to the NetBlazer. Otherwise, perform the following steps to make a backup copy of your NetBlazer system.

1. Insert your write-protected original system diskette in the NetBlazer disk drive, and enter a **diskcopy** command at the Disk command level.

```
NetBlazer:Top> disk
NetBlazer:Top>Disk> diskcopy
There will be 3 copy segments (960 blocks each, 2880 blocks total)
0% done...Insert source diskette and press return
```

2. Your original system diskette should already be in the NetBlazer disk drive. Press the return key.

```
33% done reading
Insert destination diskette and press return
```

3. Insert a blank high-density diskette into the NetBlazer disk drive, and press the return key.

4. Continue following the instructions from the NetBlazer until the following message is displayed.

```
Disk copy complete
Insert system diskette and press return
```

Use the duplicate diskette as a working copy and put the original NetBlazer system diskette away in a safe place.

5. Make sure that you have your working copy of the system diskette inserted in the disk drive, then press the return key at the above prompt.

Assigning a Host Name to the NetBlazer

The next example shows you how to assign a host name to the NetBlazer.

```
NetBlazer:Top> hostname jade
jade:Top>
```

The host name you choose, jade in the above example, is displayed as part of the command prompt.

Setting the Current Date and Time

Enter a **time** command to display the NetBlazer's current date and time.

```
jade:Top> time
Current time is Mon Nov 16 12:51:51 1992
```

If the date and time displayed is not correct, enter **settime** at the command prompt to change the setting.

```
jade:Top> settime
```

The NetBlazer prompts you for the current date and time as shown below.

```
Current time is Mon Nov 16 12:52:24 1992
[you may enter a non-numeric value (e.g. "cancel") to cancel data entry]
Enter the year [92]:
Enter the month number (1 to 12) [11]:
Enter the day of the month (1 to 30) [16]:
Enter the hour (0 to 23) [12]:
Enter the minute (0 to 59) [52]:
Enter the current second (0 to 59) [24]:
```

Parameters shown in square brackets indicate the current setting. If the value shown is correct, press the return key to accept the current value; otherwise enter the correct value.

Setting the Root Password

Set the root password by entering the following command.

```
jade:Top> passwd
Changing password for root
New Password:
Retype Password:
```

The password is not displayed on the screen as you type it, so the NetBlazer prompts you to enter the password twice to ensure that you enter it correctly.

Enter a **user list** command to display a list of current users.

```
jade:Top> user list
USERID        PASSWORD        CRYPTO            USE        PRIVS     DEST-GROUP CMD
root          tNI9TBjdZH/bM                     login      SCDRT
(PRIVS: S=status, C=config, D=dial-ok,
         T=telnet/rlogin-ok, A=acs-ok, B=ARA-ok, N=from-network)
```

Only the root user ID record is displayed at this time. The password is encrypted to prevent unauthorized viewing. Also notice that the root user ID has full system status and configuration privileges as indicated in the PRIVS field.

Verify that you can log into the NetBlazer using the new root password by issuing a **logout** command and then logging back into the NetBlazer. If you cannot log back in, reboot the NetBlazer by pressing the reset button on the NetBlazer front panel.

Saving the NetBlazer System Configuration

Make sure that you have your working copy of the NetBlazer system diskette inserted in the drive, and enter **save** at the command prompt to save the NetBlazer configuration and password file to diskette.

```
jade:Top>Configure>User> save
Saved startup file 'startup.cnf'.
Saved passwd file 'passwd'.
```

Anytime you modify the NetBlazer's current configuration, you should use the **save** command to update the STARTUP.CNF and PASSWD files on your NetBlazer system diskette.

What's Next

You are now at the point where you must decide which protocols and what functions within those protocols you wish to configure.

Protocol	Function	Reference Chapter
AppleTalk	– local router – modem server – wide area router – ARA server	16
IP	– local router – wide area router – modem server – terminal server – network management	4 and 9 5, 6, and 7 10 11 14
IPX	– local router – wide area router – modem server (ACS option required) – remote control server (ACS option required)	15

The next chapter provides some general guidelines and tips for planning the configuration. Before continuing, study this chapter and make sure that you have the information required to complete the configuration.

Because the NetBlazer can route IP, IPX, or AppleTalk packets through three types of interfaces (LAN, Dedicated, and Dynamic), an understanding of NetBlazer interface concepts is essential in order to perform a successful configuration. These concepts are explained in Chapter 2, NetBlazer Interface Descriptions.

NetBlazer™

IP Configuration

Interface

en0 - 199.171.38.1

ounet - 137.39.221.98 (LINC A)

domain

137.39.1.3

192.48.96.20

IP Router Configuration 4

This chapter provides instructions on how to configure the NetBlazer to route IP packets between local networks.

To configure the NetBlazer to route IPX or AppleTalk packets, refer to Chapter 15, IPX Configuration, and Chapter 16, AppleTalk Configuration.

To configure the NetBlazer as an IP router, each Ethernet and/or Token Ring interface must be assigned an unused address from the subnet address space of the LAN segment connected to the interface.

For example, the NetBlazer named jade in Figure 4-1 is connected to the 143.191.11.X and 143.191.63.X subnets through the en0 and en1 interfaces, respectively. Each interface is assigned an IP address from its corresponding subnet address space. Because the NetBlazer's global IP address can match one of the interface addresses, we decided to use the address assigned to the en0 interface as the global address for jade.

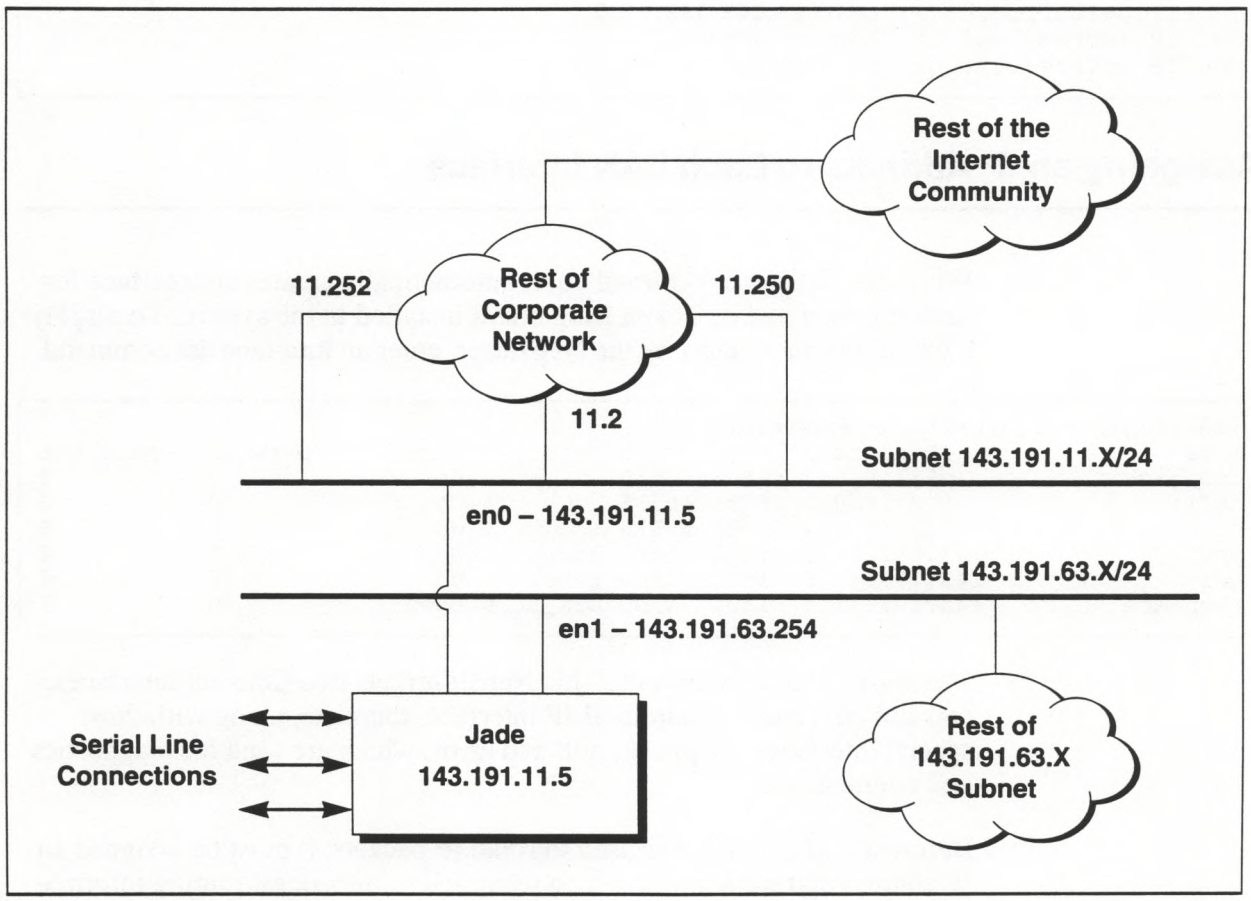


Figure 4-1. Local IP Network Example

You also need to decide how the NetBlazer will learn the routes to other LANs, which are not directly accessible to the NetBlazer. You have two choices: manually add static routes to the NetBlazer's routing table or configure the NetBlazer to dynamically learn the routes to other indirect networks using RIP (Routing Information Protocol).

Tip: *Static routes work best for small stable networks with just a few routes. For complex networks with many paths, like the network shown in Figure 4-1, RIP provides a more flexible and easier way to maintain the list of routes used by the NetBlazer.*

The remainder of this chapter describes how to configure the NetBlazer shown in Figure 4-1 to route IP packets between LANs.

Assigning a Global IP Address to the NetBlazer

Go to the Configure IP command level, and enter the global IP address assigned to the NetBlazer.

```
jade:Top>Configure> ip
jade:Top>Configure>IP> address 143.191.11.5
Set IP address(es) of 3 interface(s)
Set IP address(es) of 10 lines(s)
```

Assigning an IP Address to Each LAN Interface

When the NetBlazer is turned on, it automatically creates an interface for each Ethernet and/or Token Ring board installed in the system. To display a list of interfaces used by the NetBlazer, enter an **interface list** command.

```
jade:Top>Configure>IP> interface list
Name                IP address   MRU   MTU type     line      pkts in   pkts out
loopback             127.0.0.1 65535 65535          Up              0          0
null                 127.0.0.2 65535 65535          Up              0          0
error                127.0.0.3 65535 65535          Up              0          0
en0               143.191.11.5  1500  1500 Ether    Up              0          0
en1               143.191.11.5  1500  1500 Ether    Up              0          0
tbupdate          143.191.11.5  1500  1500 DYN_SLIP Down            0          0
```

The above display shows that this NetBlazer has two Ethernet interfaces, en0 and en1, and a dynamic SLIP interface, tbupdate, along with three special interfaces, loopback, null and error, which are used for diagnostics and maintenance.

Before a LAN interface is used to route IP packets, it must be assigned an IP address and static route. When using RIP to broadcast routing information to other routers, an ARP broadcast address must also be entered for each network segment connected directly to the NetBlazer.

Fortunately, only one command per interface provides the NetBlazer with enough information to automatically configure each interface, as illustrated below.

```
jade:Top>Configure>IP> address 143.191.11.5/24 en0
adding new route 143.191.11.5/24 en0
Set IP address of interface 'en0'
jade:Top>Configure>IP> address 143.191.63.254/24 en1
adding new route 143.191.63.254/24 en1
Set IP address of interface 'en1'
```

These commands assign IP addresses 143.191.11.5 and 143.191.63.254 to the en0 and en1 interfaces, respectively.

The **/24** at the end of each of the IP addresses is a subnet bit mask indicating that the first 24 bits are to be treated as the network part of the IP address. The NetBlazer uses this information to automatically create a static route and ARP broadcast address for each interface. If a subnet bit mask is not entered, the NetBlazer will not create a static route or ARP broadcast entry for the specified interface.

To see the effects of the above two **ip address** commands, produce listings of the interfaces, local routes, and ARP entries, as shown below.

```
jade:Top>Configure>IP> interface list
Name                IP address   MRU   MTU type     line      pkts in   pkts out
loopback             127.0.0.1 65535 65535          Up              0          0
null                 127.0.0.2 65535 65535          Up              0          0
error                127.0.0.3 65535 65535          Up              0          0
en0               143.191.11.5  1500  1500 Ether    Up              0          1
en1             143.191.63.254  1500  1500 Ether    Up              0          1
tbupdate          143.191.11.5  1500  1500 DYN_SLIP Down            0          0
jade:Top>Configure>IP> route listlocal
Dest            Len Interface    Gateway          Metric  P Timer  Use
143.191.20.1    32  tbupdate                      1       P 0      0
127.0.0.1       32  loopback                      1       P 0      0
143.191.11.0    24  en0                           1         0      0
143.191.63.0    24  en1                           1         0      0
jade:Top>Configure>IP> arp list
received 142 badtype 0 bogus addr 0 reqst in 142 replies 0 reqst out 4
IP addr         Type  Interface   Time Q Addr
143.191.63.255  ether any         0      ff:ff:ff:ff:ff:ff
143.191.11.255  ether any         0      ff:ff:ff:ff:ff:ff
```

Configuring the NetBlazer to Use RIP and/or Static Routes

To send IP packets to LAN segments that are not connected directly to one of the NetBlazer's interfaces, the NetBlazer must know which interface and gateway to use to reach a particular destination network. This information is kept in the NetBlazer's IP routing table, which includes two types of entries: static routes manually entered by an operator and acquired routes added to the routing table by RIP advertisements from other routers on the network.

Using RIP (Routing Information Protocol)

The NetBlazer is shipped with the RIP server turned on, which allows it to accepts routing information from other routers on the network. If your NetBlazer is connected to a subnet with another router that is broadcasting RIP information, entering a **route list** command shows entries in the routing table that were added to the table by RIP.

If you do not want the NetBlazer to accept routing information from other routers on its LANs, you can turn the RIP server off by issuing a **server stop rip** command. Use a **rip refuse** <IP-address> command to stop the NetBlazer from accepting RIP information from one specific router.

If you want the NetBlazer to broadcast RIP information to other routers on its LANs, go to the Configure IP RIP command level and add a RIP broadcast address for each LAN segment connected directly to the NetBlazer.

```
jade:Top>Configure>IP> rip
jade:Top>Configure>IP>RIP> add 143.191.11.255 30 yes
jade:Top>Configure>IP>RIP> add 143.191.63.255 30 yes
```

These commands cause the NetBlazer to send RIP information to each LAN's broadcast address in 30 second intervals. The last parameter (yes) in each entry tells the NetBlazer to use split horizons, which tends to make the routing tables converge more rapidly when a router is no longer in service.

Enter **list** at the Configure IP RIP command level to verify your entries.

```
jade:Top>Configure>IP>RIP> list
RIP statistics:
 Total sent:          17    Total rcvd:       14401    Reqst sent:           0
 Reqst recd:           0    Resp sent :          17    Resp recd :       14401
 Unknown pkts recd:            0     Refused pkts:           0
Active RIP output interfaces:
Dest Addr       Interval Split
143.191.63.255  30       1
143.191.11.255  30       1
```

Setting Up Static Routes to Indirect Networks

You normally only need to set up static routes to indirect LANs (those LANs that are not connected directly to the NetBlazer) if you are not using RIP to dynamically maintain the routing table.

The **route add** or **route addprivate** commands are used to set up static routes. If you are using RIP and do not want a particular route advertised by RIP, use **route addprivate**. Otherwise, use the **route add** command. These two commands use the following syntax:

route add <dest_addr>[/<bits>] <interface> [<gateway> <metric>]
route addprivate <dest_addr>[/<bits>] <interface> [<gateway> <metric>]

Both commands require a destination IP address, a subnet bit mask, and an interface name. A gateway IP address and metric is also required if the destination subnet is more than one hop count away from the NetBlazer.

The following example shows you how to enter an indirect route to the 143.191.10.X subnet, which is accessible through the 143.191.11.252 gateway.

```
jade:Top>Configure>IP> route
jade:Top>Configure>IP>Route> add 143.191.10/24 en0 143.191.11.252 2
```

Use the **route lookup** command to verify that you have enter the static route correctly.

```
jade:Top>Configure>IP>Route> lookup 143.191.10/24
Dest            Len Interface    Gateway          Metric  P Timer  Use
143.191.10.0    24  en0          143.191.11.252   2         0      0
```

The new entry shows that subnet 143.191.10.X is 2 hops away from the NetBlazer, and IP packets destined for this subnet are sent to gateway 143.191.11.252 through the en0 interface.

Setting Up a Default Route

To keep the routing table small, you can create a default route, which is used to route IP packets that do not have a designated route.

Caution: *If you are using RIP, only one router should have a static default route that is advertised by RIP. The remaining routers should learn the default route from RIP or use a private default route that is not advertised to the rest of the network.*

Use the **route addprivate default** command to set up a default route, as shown in the next example.

```
jade:Top>Configure>IP>Route> addprivate default en0 143.191.11.252
adding new route default en0
```

Verify that the default route is correct by entering the following command.

```
jade:Top>Configure>IP>Route> list |grep default
default         0   en0          143.191.11.252   1        P 0      0
```

Notice that a default route has been added to the table. This default route routes all IP packets that do not have a designated route through interface en0 to gateway 143.191.11.252.

Configuring the NetBlazer as a Domain Name System Client

If your network includes one or more domain name servers, go to the Configure IP Domain command level and add the IP address for each name server to the domain server list, as illustrated below:

```
jade:Top>Configure>IP>Route> domain
jade:Top>Configure>IP>Domain> add 143.191.10.100
jade:Top>Configure>IP>Domain> list
Server address      srtt    mdev    timeout queries responses
143.191.10.100      5000    0       5030    0       0
```

As a DNS client, the NetBlazer accepts a host name in a **telnet**, **rlogin**, **ftp**, or **ping** command and queries the name server(s) identified in the domain server list for the IP address of the specified host. The IP address is then used to establish the desired connection. This allows users to enter domain names instead of IP addresses.

The **domain suffix** command, shown in the following example, allows you to define a suffix that is added to the end of any domain name supplied by the user that does not contain a dot (period). The NetBlazer treats domain names that include a dot as a complete domain name and will not add the suffix to the supplied name before querying a name server for the host IP address.

```
jade:Top>Configure>IP>Domain> suffix telebit.com
```

If the domain suffix is set to telebit.com, as shown above, and a user issues a **telnet marketing** command to the NetBlazer, the NetBlazer expands the domain name to marketing.telebit.com before requesting the IP address from a name server on the network.

Entering the **domain suffix** command without a suffix string displays the current domain name suffix.

Testing the IP Router Configuration

To verify that the NetBlazer is correctly configured to route IP packets, go to the Sessions command level and **ping** several hosts that you believe should be reachable from the NetBlazer.

```
jade:Top>Sessions> ping napa
PING napa(143.191.10.100): 64 bytes      min/avg/max/mdev
Type ^] (decimal 29) <CR> to return to NetBlazer
64 bytes from 143.191.10.100 icmp_seq=0 time=5 ms  5/5/5/0
64 bytes from 143.191.10.100 icmp_seq=1 time=5 ms  5/5/5/0
64 bytes from 143.191.10.100 icmp_seq=2 time=5 ms  5/5/5/0
```

To stop a **ping** session, hold down the **ctrl** (control) key and press the **c** key. The NetBlazer then displays the **ping** statistics.

```
----napa PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max/mdev = 5/5/5/0
```

If you did not receive the appropriate response from a **ping** session, try doing the following to isolate the problem:

- Ping another host that uses a different route to determine if the problem occurs on just one path or on several different paths.
- If you are using a domain name server, enter a **domain lookup** <hostname> command to verify that the NetBlazer can reach the domain name server and the server has an entry for the host you are trying to reach.
- Use the **route lookup** <dest-addr> command to verify that a route exists between the NetBlazer and the host you are trying to reach.
- Use the **interface trace** <interface> <options> command to examine the traffic on the specified interface.
- If you are having problems routing IP traffic to a remote site over a dial-up connection, verify that the dynamic interfaces on both sides of the link are configured correctly. Use the **line trace** <line-name> <options> command to monitor the chat dialog exchanged between the two NetBlazers while attempting to establish a connection.

Refer to the *NetBlazer Command Reference* manual for an explanation on how to use the commands mentioned above.

What's Next

To route IP packets between the local and remote sites, you must set up dedicated or dynamic serial interface links between the local and remote NetBlazers.

Instructions on how to set up a dedicated synchronous or asynchronous point-to-point link between NetBlazers are provided in the next chapter.

For instructions on how to set up dynamic dial-up connections between NetBlazers, refer to Chapter 6, Dynamic IP Interface Configuration.

Dedicated IP Interface Configuration 5

This chapter describes how to configure the NetBlazer to route IP packets between a local and remote site over a dedicated point-to-point link. Before attempting to set up a dedicated interface, read Chapter 2 to be sure that you know how dedicated interfaces are used and what information you need to set up the connection.

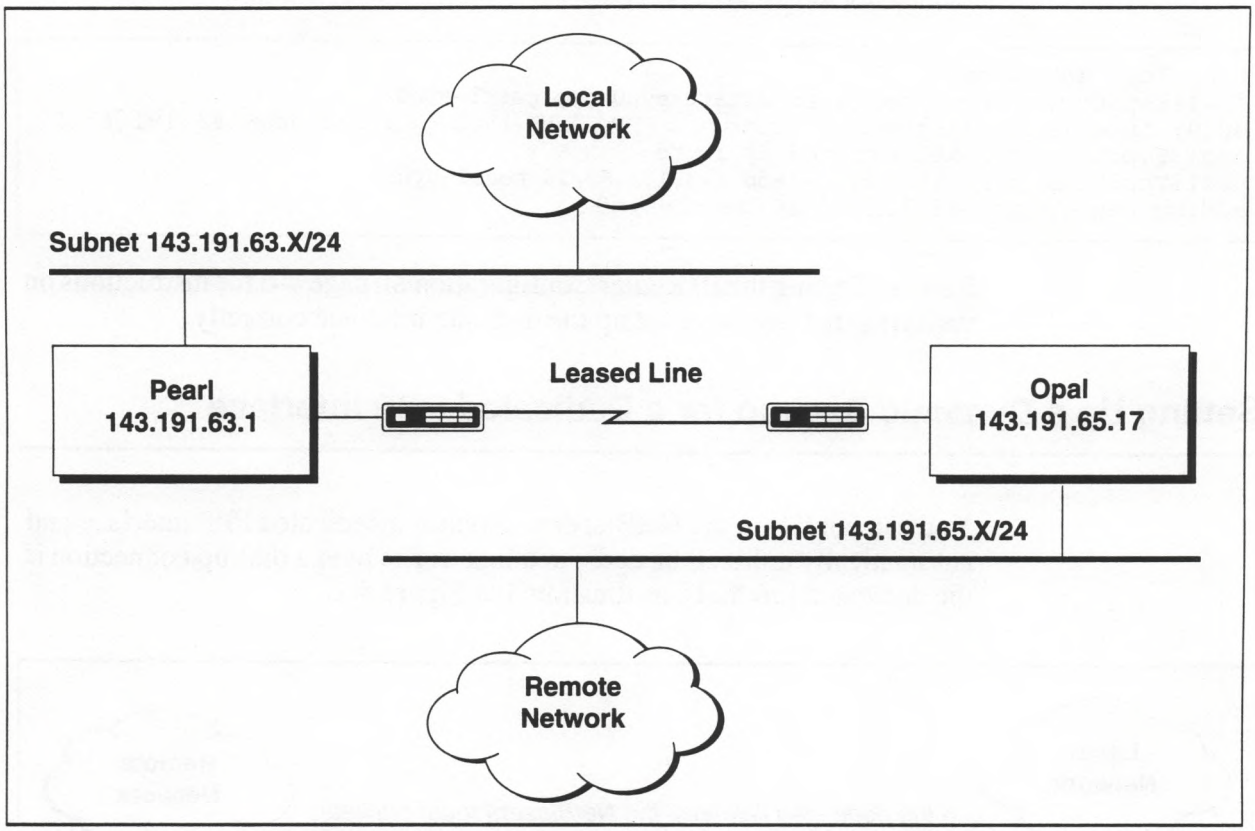


Figure 5-1. Dedicated Interface Configuration

Setting Up a Dedicated PPP Interface Link

The following procedures shows you how to set up a dedicated synchronous PPP interface link between the two NetBlazers shown in Figure 5-1.

On the local NetBlazer (pearl) enter an **interface attach** command to assign an PPP interface (opal-syn0) to the synchronous line (syn0).

```
pearl:Top> interface
pearl:Top>Configure>Interface> attach syn0 ppp opal-syn0
syn0: interface=opal-syn0, protocol=PPP, MRU=1500, ip address=143.191.63.1
```

Note: *PPP framing is required in most cases. SLIP framing may be used only for an asynchronous IP link that does not require a dial-up backup link.*

Next, add an IP route for each remote subnet to the local NetBlazers IP routing table.

```
pearl:Top>Configure>Interface> ip route
pearl:Top>Configure>IP>Route> add 143.191.65/24 opal-syn0
adding new route 143.191.65/24 opal-syn0
```

Repeat the above procedure on the remote NetBlazer (opal).

```
opal:Top> interface
opal:Top>Configure>Interface> attach syn0 ppp pearl-syn0
syn0: interface=pearl-syn0, protocol=PPP, MRU=1500, ip address=143.191.65.17
opal:Top>Configure>Interface> ip route
opal:Top>Configure>IP>Route> add 143.191.63/24 pearl-syn0
adding new route 143.191.63/24 pearl-syn0
```

Refer to Testing the IP Router Configuration on page 4-6 for instructions on verifying that you have set up the dedicate interface correctly.

Setting Up a Dynamic Backup for a Dedicated PPP Interface

You can configure the NetBlazer to monitor a dedicated PPP interface and automatically redirect the dedicated link traffic over a dial-up connection if the dedicated link fails, as illustrated in Figure 5-2.

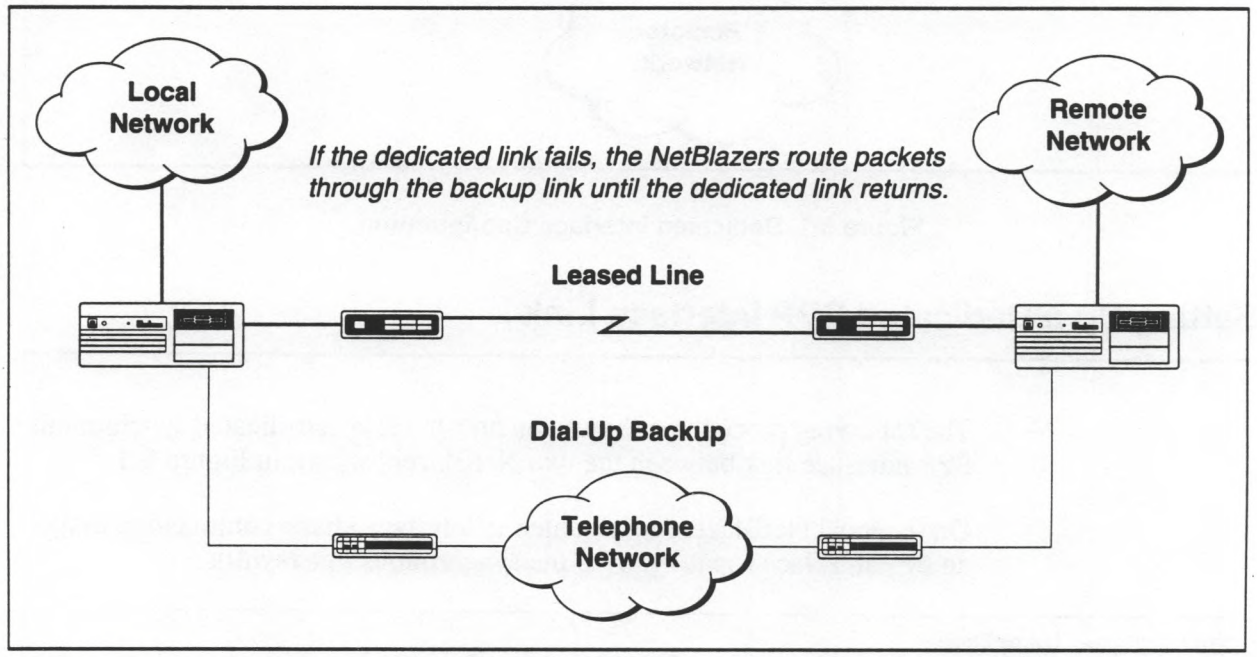


Figure 5-2. Dial-Up Backup for a Dedicated PPP Link

Perform the following procedure to set up a dial-up backup for a dedicated PPP link.

Use **pppdial** or **ipdial** to set up a dynamic interface on the local NetBlazer.

```
pearl:Top> dynamic pppdial
Name of the remote (other) system: opal
Phone number: 9-555-1234
Authentication method (crypto, password, none) [c]:
Enter the crypto key (no echo):
Re-enter the crypto key:
Add dialout 'opal'
Add user 'opal'
Add dynamic interface=opal, user=pearl chat=ics, with crypto handshaking
 using PPP, MRU=1500
Okay (yes|no|quit) [y]?
REMINDER! You need to set up route(s) for this interface
```

Note: *Do **not** enter routes through the dynamic interface.*

Assign the dynamic backup interface to the dedicated interface by entering an **interface backup** <interface> <backup_interface> command.

```
pearl:Top> interface backup opal-syn0 opal
```

Start a watchdog server for the dedicated interface by entering a **server start watchdog** <interface> [<seconds>] command.

```
pearl:Top> server start watchdog opal-syn0
```

The watchdog tests the dedicated link at specified intervals (the default is every 120 seconds). If the watchdog detects a failure on the dedicated link, the NetBlazer establishes a dial-up connection to the remote site through the backup interface and switches the dedicated interface routes to the backup interface. When the dedicated link returns, the NetBlazer drops the dial-up connection and returns the original routes through the dedicated interface.

Repeat the above procedure on the other side of the link.

```
opal:Top> dynamic pppdial
Name of the remote (other) system: pearl
Phone number: 9-555-9876
Authentication method (crypto, password, none) [c]:
Enter the crypto key (no echo):
Re-enter the crypto key:
Add dialout 'pearl'
Add user 'pearl'
Add dynamic interface=pearl, user=opal chat=ics, with crypto handshaking
 using PPP, MRU=1500
Okay (yes|no|quit) [y]?
REMINDER! You need to set up route(s) for this interface
opal:Top> interface backup pearl-syn0 pearl
opal:Top> server start watchdog pearl-syn0
```

Dynamic IP Interface Configuration 6

This chapter describes how to configure the NetBlazer to route IP packets between a local and remote site over the public telephone network. Before attempting to set up a dynamic interface, read Chapter 2 to be sure that you know how dynamic interfaces are used and what information you need to set up dynamic connection.

You can configure the NetBlazer to route IP traffic over a single dynamic interface connection; or if you require greater throughput, you can configure the NetBlazer to distribute IP traffic over multiple dynamic connections to the remote site. Refer to page 6-4 for instructions on how to set up load balancing over multiple connections.

Setting Up a Single-Line Dynamic Interface

The following example illustrates how to set up a single-line PPP interface between the two NetBlazers, jade and ruby, shown in Figure 6-1.

```
jade:Top> dynamic
jade:Top>Configure>Interface>Dynamic> pppdial
Name of the remote (other) system: ruby
```

Be sure to enter the hostname of the remote NetBlazer because the local NetBlazer uses this name during the authentication process when establishing a connection with the remote site.

```
Phone number: 9-555-1234
```

Enter the telephone number of the remote connection. Refer to the **Dial** command description in your modem's reference manual for a description of acceptable dial strings.

```
Authentication method (crypto, password, none) [c]:
```

Select the authentication method to use when establishing a connection with the remote site. For NetBlazer to NetBlazer connections, a crypto challenge and response is best.

```
Enter the crypto key (no echo):
Re-enter the crypto key:
```

The crypto key is not displayed as you type it, so you are asked to enter the crypto key twice to ensure that you entered it correctly.

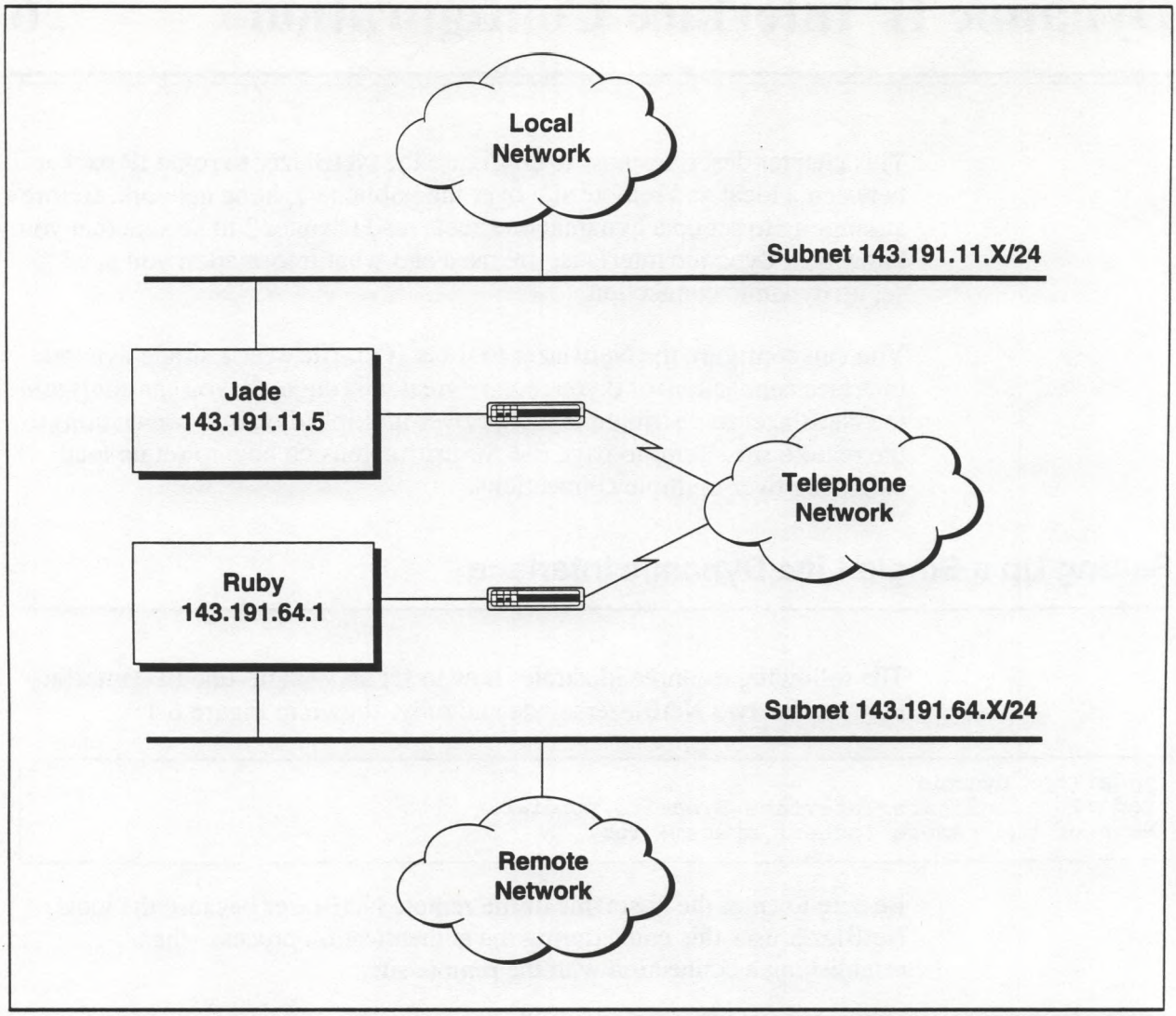


Figure 6-1. Single Line Dynamic Interface Configuration

```
Add dialout 'ruby'
Add user 'ruby'
Add dynamic interface=ruby, user=jade chat=ics, with crypto handshaking
 using PPP, MRU=1500
Okay (yes|no|quit) [y]?
```

Press the return key or enter **y** to confirm that you want to create the dial-out, user, and interface records.

```
REMINDER! You need to set up route(s) for this interface
```

After you have set up the interface, you must add an IP route for each subnet at the remote site to the NetBlazer's IP routing table.

Note: *If you want the routes to the network to be available only when a connection is established from the remote site, you can choose to not add static routes and use the* ***dynamic auto-route*** *command to set up temporary routes to the remote network(s) instead.*

Go to the IP Route command level and add one or more static routes for this interface.

```
jade:Top>Configure>Interface>Dynamic> ip route
jade:Top>Configure>IP>Route> add 143.191.64/24 ruby
adding new route 143.191.64/24 ruby
```

At this point you are halfway finished. You must set up a dynamic interface on the remote NetBlazer to complete the job. If the remote NetBlazer is installed and ready to accept calls, you can use the **dial** command to call the remote NetBlazer and run **pppdial** from your local NetBlazer as illustrated below. Be sure to enter the same crypto key (or password) that you used for the local NetBlazer.

```
jade:Top>Configure>IP>Route> session
jade:Top>Sessions> dial ruby
Trying ruby(9-555-1234):dialout on line10 ... connected


Type ^] (decimal 29) <CR> to return to NetBlazer
Connected to ruby


Telebit's NetBlazer Version 2.0

ruby login: root
Password:

ruby:Top> dynamic
ruby:Top>Configure>Interface>Dynamic> pppdial
Name of the remote (other) system: jade
Phone number: 9-555-9876
Authentication method (crypto, password, none) [c]:
Enter the crypto key (no echo):
Re-enter the crypto key:
Add dialout 'jade'
Add user 'jade'
Add dynamic interface=jade, user=ruby chat=ics, with crypto handshaking
 using PPP, MRU=1500
Okay (yes|no|quit) [y]?
REMINDER! You need to set up route(s) for this interface
ruby:Top>Configure>Interface>Dynamic> ip route add 143.191/16 jade
adding new route 143.191/16 jade
ruby:Top>Configure>Interface>Dynamic> logout
jade:Top>Sessions>
```

Refer to Testing the IP Router Configuration on page 4-6 for instructions on verifying that you have set up the dynamic interface correctly.

This section describes how to set up multiple interfaces with load balancing to increase the overall throughput between the local and remote sites.

As illustrated in Figure 6-2, you must set up a pair of dynamic interfaces for each dial-up connection between the local and remote NetBlazers. In this example, ruby-s1 to jade-s1 forms one connection, and ruby-s2 to jade-s2 forms the second connection in a two-line dial-up link between the two sites. IP traffic traveling across the link is distributed across both connections, thereby increasing the maximum throughput of the link.

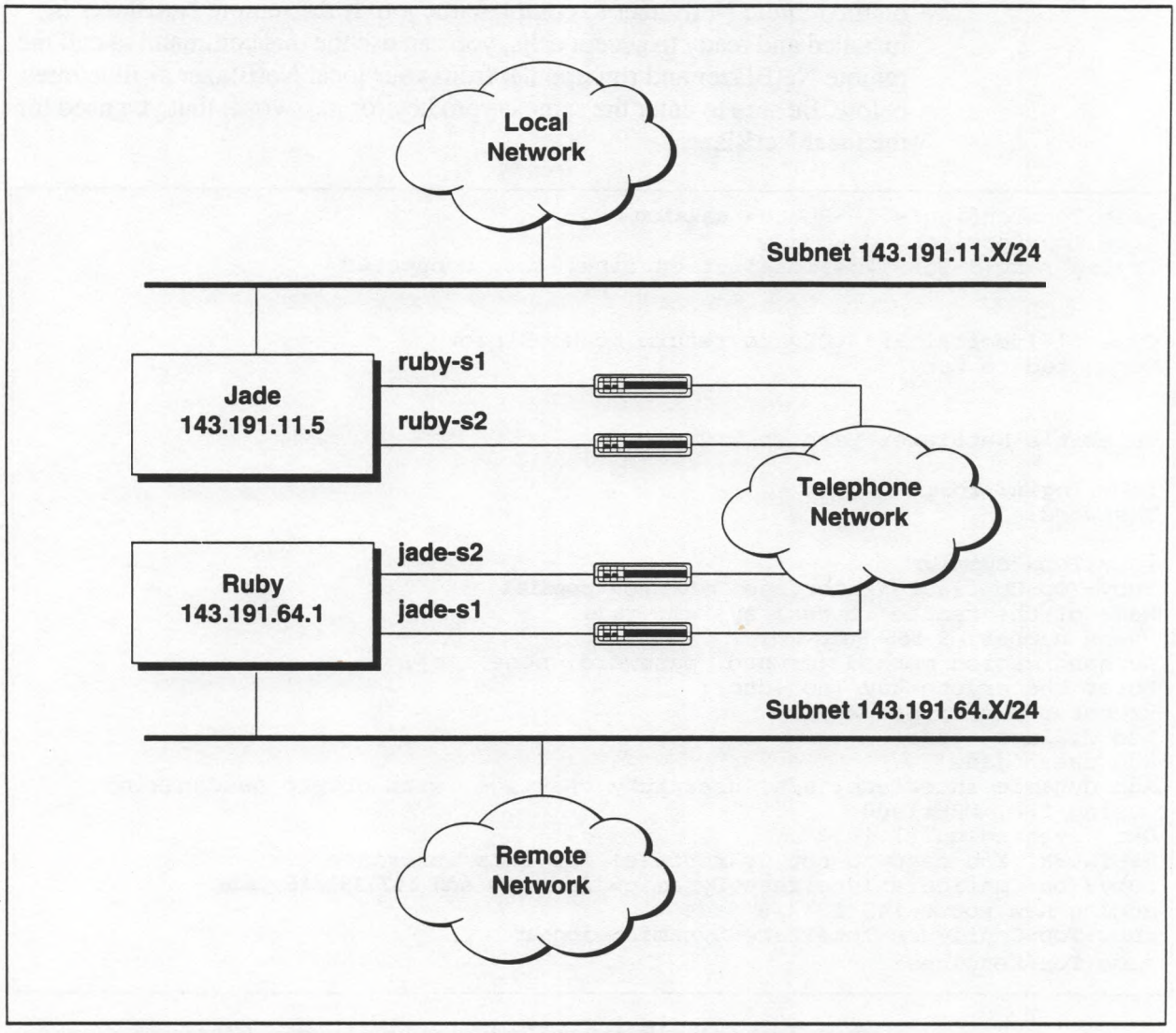


Figure 6-2. Multiple Interface Connection

General Guidelines

To set up a multiline load balanced link between two NetBlazers, perform the following steps:

1. Make sure that you have all of the information required to set up each dynamic connection in the link (refer to Table 6-1).

2. Use the **dynamic ipdial** command to set up the dynamic interfaces on each side of each dial-up connection. When setting up the dynamic interfaces, observe the following guidelines:

   a. When choosing names for the interfaces on one side of the link, consider using the name of the NetBlazer on the opposite side of the link as part of the interface name.

   b. Unless security is a major concern, use the same password or crypto key in both the user and dial-out records for all interfaces in the balanced group. This helps ensure that the authentication information exchanged between the local and remote NetBlazers matches up correctly.

   c. Only enter one telephone number per interface. If several remote sites will be calling into your central site, have your PBX service provider set up a hunt group for the modems at the central site.

   d. Use the same framing protocol (SLIP or PPP) for all interfaces.

   e. If you are using SLIP, set the MRU/MTU to 256. If you are using PPP, set the MRU to 1500 and set the MTU to 256.

   f. Only add route(s) for the first interface created on each side of the link, and use the **ip route balance** command to assign the route(s) to the other interfaces in the group.

   g. Make sure that each route's destination address is fully qualified with a bit mask.

3. Use the **ip route balance** command to set up balanced routes for each subnet on the opposite side of the link. To use load balancing in both directions, you must issue a **ip route balance** command on both sides of the link.

4. To optimize TCP performance across a multiline link, enter a **dynamic queue-max** <interface> **64** command for each interface in a balanced route.

5. If you want to delay bringing up all of the lines until the traffic through the first connection warrants it, issue an **interface mdelay** command for each interface in a balanced route.

6. Test the link by using FTP to transfer a large file from a host on one side of the link to another host on the opposite side of the link.

Table 6-1. Multiline Dynamic Interface Configuration

Field	Local NetBlazer	Remote NetBlazer
Interface name	User ID expected from remote site	User ID expected from local site
Creating a Dial-in User Record		
Password	Password expected from remote site	Password expected from local site
Crypto key	Crypto key used to authenticate crypto response from remote NetBlazer	Crypto key used to authenticate crypto response from local NetBlazer
Creating a Dial-out Record		
Phone number	Phone number of remote NetBlazer	Phone number of local NetBlazer
Line characteristics	dialout (default)	dialout (default)
User name	User ID sent to remote NetBlazer	User ID sent to local NetBlazer
Password	Password sent to remote NetBlazer	Password sent to local NetBlazer
Crypto key	Crypto key used by local NetBlazer to generate crypto response	Crypto key used by remote NetBlazer to generate crypto response
Chat script	ics (default)	ics (default)
Creating the Interface Record		
Framing	SLIP (default)	SLIP (default)
MRU/MTU	256	256
Adding Route(s)		
Address/bits	IP address of remote subnet	IP address of local subnet
Metric	Number of hops to subnet	Number of hops to subnet
Private	No (default)	No (default)

Using Ipdial to Set Up a Dynamic Interface

Go to the Interface Dynamic command level and enter **ipdial**.

```
jade:Top> dynamic
jade:Top>Configure>Interface>Dynamic> ipdial
```

This routine steps you through the process of setting up a user account, dial-out record, interface record, and one or more routes to the remote site.

```
Interface name: ruby-s1
```

This name is assigned to the dynamic interface. It is also used to create a user and/or dial-out record. Because this name is used to authenticate a dial-in connection, enter the user ID that you expect from the remote site.

```
Do you want to allow dial-in to this interface [y]?
```

Press the return key or enter **y** to create a user record with the same name as this interface.

```
Please provide the information that the remote system 'ruby-s1'
        will use to contact this NetBlazer
This info will be used to create a new user account on this NetBlazer.
Want to enter a password [y]?
```

If you intend to have the NetBlazer issue a crypto challenge, entering a password is not necessary. In this case, you can enter **n** to the above prompt. However, if you want to use a password to authenticate a dial-in connection from the remote site, press the return key or enter **y** to the prompt.

```
Enter the password (no echo):
Re-enter the password:
```

The above password prompts allow you to specify the password that is required from the remote system. The password is not displayed on the screen as you type it, so you are asked to enter the password twice to ensure that you entered it correctly.

```
Issue a crypto handshake [n]? y
```

Enter **y** to issue a crypto challenge to a remote system that attempts to establish a connection through this interface.

```
Enter the crypto key (no echo):
Re-enter the crypto key:
```

Enter the crypto key that is used to authenticate a crypto response sent by the remote system when a crypto challenge is issued. The remote NetBlazer must have an identical crypto key in its dial-out record to allow a successful connection. The crypto key is not displayed on the screen as you type it, so you are asked to enter the crypto key twice to ensure that you entered it correctly.

```
User: ruby-s1              privs:          dest-group:
Okay (yes|no|quit) [y]?
```

Press the return key or enter **y** to create the specified user record. Otherwise, enter **n** to discard this user record and start a new user record, or enter **q** to abort this dynamic interface and return to the command prompt.

```
Do you want to allow dial-out from this interface [y]?
```

To allow a dial-out connection with the remote site through this interface, press the return key or enter **y** in response to the above prompt.

```
Begin adding dial-out 'ruby-s1' ...
Phone number: 9-555-1234
```

Enter the telephone number of the remote connection. Refer to the **Dial** command description in your modem's reference manual for a description of acceptable dial strings.

```
Line characteristics [dialout]:
```

Enter an existing characteristics group name or press the return key to accept the default characteristics group (dialout). This entry is used to select a serial line with the same characteristics when placing a call to the remote site. If no line is available with the specified characteristics, the call is not placed.

```
Adding new dialout: name=ruby-s1, phone=9-555-1234, characteristics=dialout
Okay (yes|no|quit) [y]?
```

Press the return key or enter **y** to create a dial-out record with the phone number and line characteristics specified. Otherwise, enter **n** to discard this dial-out record and start a new dial-out record, or enter **q** to abort this dynamic interface and return to the command prompt.

```
Add another dial-out [n]?
```

Answering **y** to the above prompt allows you to create another dial-out record for this interface. However, because we are setting up a dynamic interface for a multiline link, we only want one dial-out record per interface. Press the return key or enter **n** at the above prompt.

```
User ID to send to remote system [jade]: jade-s1
```

The above prompt allows you to enter the user ID that is sent to the remote site to establish a dial-out connection. The remote NetBlazer must have a corresponding user ID in its user records to allow a connection. If you enter a password and/or crypto key, the remote user record must also include a matching password and/or crypto key.

```
Want to enter a password [y]?
```

If you want to use a password to authenticate the connection, press the return key or enter **y** to the prompt.

```
Password to send to remote system (no echo):
Re-enter the password:
```

The password is not displayed on the screen as you type it, so you are asked to enter the password twice to ensure that you entered it correctly.

```
Will remote system issue a crypto handshake [n]? y
```

Crypto handshaking adds another level of security when attempting to connect with the remote system. Enter **y** to use crypto handshaking.

```
Enter the crypto key (no echo):
Re-enter the crypto key:
```

Enter the crypto key that is used to encrypt the response to a crypto challenge sent from the remote NetBlazer. The crypto key is not displayed on the screen as you type it, so you are asked to enter the crypto key twice to ensure that you entered it correctly.

```
Chat script [ics]:
```

This prompt allows you to assign a chat script to the dial-out record. Press the return key to accept the default chat script supplied with the NetBlazer.

Creating the Interface Record

```
Begin adding interface 'ruby-s1' ...
SLIP or PPP (s|p) [s]:
```

When setting up a multiline interface with load balancing, choose SLIP framing unless you have a reason to do otherwise. Press the return key or enter **s** to select SLIP framing.

```
What is the Maximum Receive Unit (MRU) [1006]: 256
```

To achieve the best performance through a load-balanced interface, set the MRU/MTU to 256.

```
Add dynamic interface=ruby-s1, user=jade-s1 chat=ics, with crypto
handshaking
 using SLIP, MRU=256
Okay (yes|no|quit) [y]?
```

Press the return key or enter **y** to create the specified interface record. Otherwise, enter **n** to discard this interface record and start a new interface record, or enter **q** to abort the interface and return to the command prompt.

Adding Routes for the Remote Site

Only add route(s) for the first interface created on each side of a multi-line link. Use the **ip route balance** command to assign the route(s) to the other interfaces in the group.

```
Add routes for interface [y]?
```

Press the return key or enter **y** at the prompt to add one or more static IP routes to the routing table.

```
Begin adding route thru 'ruby-s1' ...
Destination name or address/bits (Return to finish routes): 143.191.64/24
```

Enter the IP address and subnet bit mask for the remote network. The **/24** in the above example is a subnet bit mask indicating that the first 24 contiguous bits are to be treated as the network part of the IP address.

```
Metric [1]:
```

Enter the number of hops required to reach the destination network.

```
Private [n]:
```

If you do not want this network advertised through RIP, enter **y** at the prompt. Otherwise, press the return key or enter **n** to allow RIP to advertise this route to the rest of the network.

```
Add route destination=143.191.64.0, bits=24, metric=1, not private
Okay (yes|no|quit) [y]?
```

Press the return key or enter **y** to create the route. Otherwise, enter **n** to discard this route, or enter **q** to abort this interface and return to the command prompt.

```
Route added
Begin adding route thru 'ruby-s1' ...
Destination name or address/bits (Return to finish routes):
```

Repeat the above route add procedure for each subnet at the remote site that you want to be accessible through this interface.

When you have finished entering routes for all subnets at the remote site, press the return key to exit the **ipdial** routine.

Checking the Interface Configuration

The NetBlazer displays information describing how a connection to the remote site is established through this interface.

```
... Done adding ruby-s1.
Make sure Remote and Local agree on password and crypto key

Dynamic interface=ruby-s1, framing=SLIP MRU=256 (therefore remote MTU<=256)

Outbound Call Setup - To dial out this host (jade) will do the following:
        dial phone number(s):  9-555-1234
        invoke the chat script (ics) to send username=jade-s1, password=passport
        will use key=cipher to respond to crypto challenge from remote

        Routes via ruby-s1:
Dest            Len Interface    Gateway          Metric  P Timer  Use
143.191.64.0    24  ruby-s1                       1         0      0

Inbound Call Setup - When a call comes in this host (jade) prompts:
                login:
Remote sends
                ruby-s1
this host (jade) prompts:
        password:
                (Remote sends the password you assigned to ruby-s1)
        this host (jade) will issue a challenge
        Remote uses the crypto key to encrypt the challenge and send it back

        Remote needs route to this host (jade)
```

This information helps you determine how to set up the dynamic interface on the other side of the connection. You can review the above information at a later time by issuing a **dynamic farside** <interface> command.

Setting Up the Remote Interface

After setting up a dynamic interface on the local NetBlazer, you must do the same thing on the remote NetBlazer. If the remote NetBlazer is installed and ready to accept calls, you can use the **dial** command to call the remote NetBlazer and run **ipdial** from your local NetBlazer.

When a character mode connection is established, log in as root or some other user with system configuration privileges. Then use **ipdial** to set up the remote interface using the reciprocal values of the local interface. The remote NetBlazer's interface name and user record must match the user name, password, and/or crypto key entered in the local NetBlazer's dial-out record. Likewise, the remote NetBlazer's dial-out record must match the local NetBlazer's interface name and user record.

Setting Up Balanced Routes

To route IP traffic for a specified destination through two or more interfaces, enter a **balance** command at the IP Route command level.

```
jade:Top>Configure>Interface>Dynamic> ip route
jade:Top>Configure>IP>Route> balance 143.191.64/24 ruby-s1 ruby-s2
```

The above **ip route balance** command configures the NetBlazer to route IP traffic destined for 143.191.64/24 through interfaces ruby-s1 and ruby-s2.

Use the **ip route listbalance** and **listlocal** commands to verify that the routes to the remote site are correct.

```
jade:Top>Configure>IP>Route> listbalance
Dest            Len Interface    Gateway          Metric  P Timer  Use
143.191.64.0    24  ruby-s1                       1          0      0
143.191.64.0    24  ruby-s2                       1          0      0
jade:Top>Configure>IP>Route> listlocal |grep ruby
143.191.64.0    24  ruby-s1                       1          0      0
143.191.64.0    24  ruby-s2                       1          0      0
```

To optimize TCP performance across a multiline link, set each interface's queue-max to 64.

```
jade:Top>Configure>IP>Route> dynamic
jade:Top>Configure>Interface>Dynamic> queue-max ruby-s1 64
jade:Top>Configure>Interface>Dynamic> queue-max ruby-s2 64
```

If you want to delay bringing up all of the lines until the traffic through the first connection warrants it, issue an **interface mdelay** command for each interface in a balanced route.

```
jade:Top>Configure>Interface>Dynamic> interface
jade:Top>Configure>Interface> mdelay ruby-s1 120 20
jade:Top>Configure>Interface> mdelay ruby-s2 120 20
```

The above **interface mdelay** commands configure the NetBlazer to delay bringing up more than one connection until the first connection's total traffic divided by its expected capacity exceeds 20% (the default threshold) over a 120 second (2 minute) interval. Refer to the **interface mdelay** command description in the *NetBlazer Command Reference Manual* for additional instructions on choosing the best **mdelay** interval and threshold settings.

To use load balancing in both directions, repeat these procedures on the other side of the link.

If you want the local NetBlazer's IP routing table to include routes to the remote site only when a dial-in connection is established from the remote site, use the **dynamic auto-route** command to assign one or more auto-routes to a dynamic interface instead of adding static routes to the routing table.

For example, assume that you want the remote subnets shown in Figure 7-1 to be accessible only when a dial-in connection has been established from the remote site through the dynamic interface named ruby.

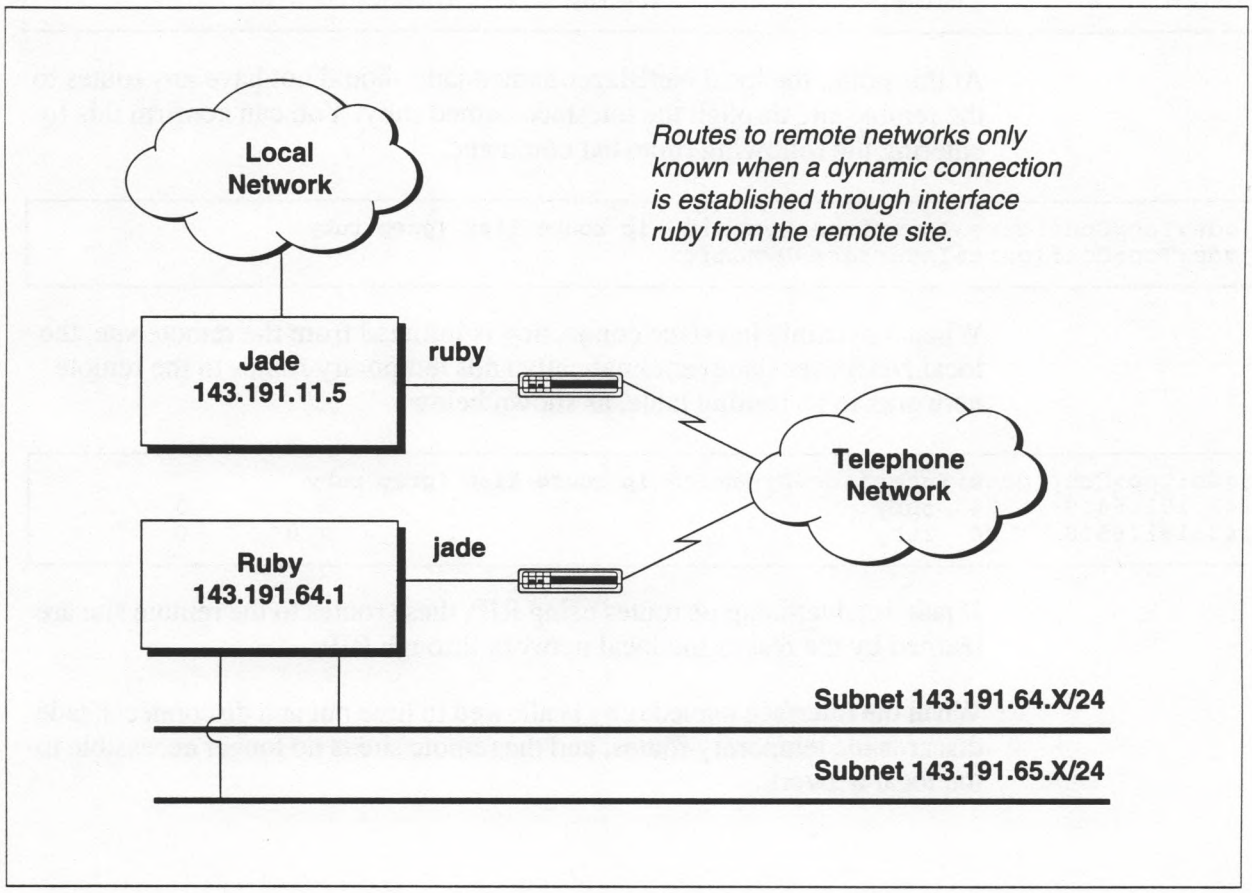


Figure 7-1. Auto-Route Example

First, use **pppdial**, **slipdial** or **ipdial** to create dynamic interfaces for ruby and jade as described in Chapter 6. *Do not enter any static routes to the remote site on the local NetBlazer named jade.*

Next, add auto-routes for the networks at the remote site to the dynamic interface named ruby.

```
jade:Top>Configure>Interface>Dynamic> auto-route ruby add 143.191.64/24
jade:Top>Configure>Interface>Dynamic> auto-route ruby add 143.191.65/24
jade:Top>Configure>Interface>Dynamic> list ruby
Name              IP address   MRU   MTU type     line        pkts in   pkts out
ruby           143.191.11.5  1500  1500 DYN_PPP  Down              0          0
Idle: In 4:01:42:38   Out 4:01:42:38                  IP:          0          0
Auto IP's :143.191.64.0/24 143.191.65.0/24
Will save 'ruby' vj: auto
Current vj: not active
Ip Broadcast Address 255.255.255.255    Netmask     255.255.0.0
Interface = Dynamic PPP     Uname = jade        Password = <<NONE>>
Dial-out = Yes         Dial-in = Yes
Chat script = ics      Crypto key = cipher     MRU = 1500     MTU=1500
Timeout = 180 s        Queue-max = 8
Cost = 1000         Bytespertick = 0    Mdelay = 0   Threshold = 20
```

At this point, the local NetBlazer named jade should not have any routes to the remote site through the interface named ruby. You can confirm this by entering the following **route list** command.

```
jade:Top>Configure>Interface>Dynamic> ip route list |grep ruby
jade:Top>Configure>Interface>Dynamic>
```

When a dynamic interface connection is initiated from the remote site, the local NetBlazer (jade) automatically adds temporary routes to the remote networks to its routing table, as shown below.

```
jade:Top>Configure>Interface>Dynamic> ip route list |grep ruby
143.191.64.0    24  ruby                              1       A 0       0
143.191.65.0    24  ruby                              1       A 0       0
```

If jade is advertising its routes using RIP, these routes to the remote site are learned by the rest of the local network through RIP.

When the interface named ruby is allowed to time out and disconnects, jade discards the temporary routes, and the remote site is no longer accessible to the local network.

Using Proxy ARP 8

Proxy ARP allows the NetBlazer to respond to ARP requests intended for another machine by supplying its own physical address. The NetBlazer then receives packets for that host and forwards them to the proper destination.

To illustrate how proxy ARP is used, assume that you have a host with an IP address on the same network as the NetBlazer, but you must move that host to a remote location that is accessible via a dynamic connection (see Figure 8-1).

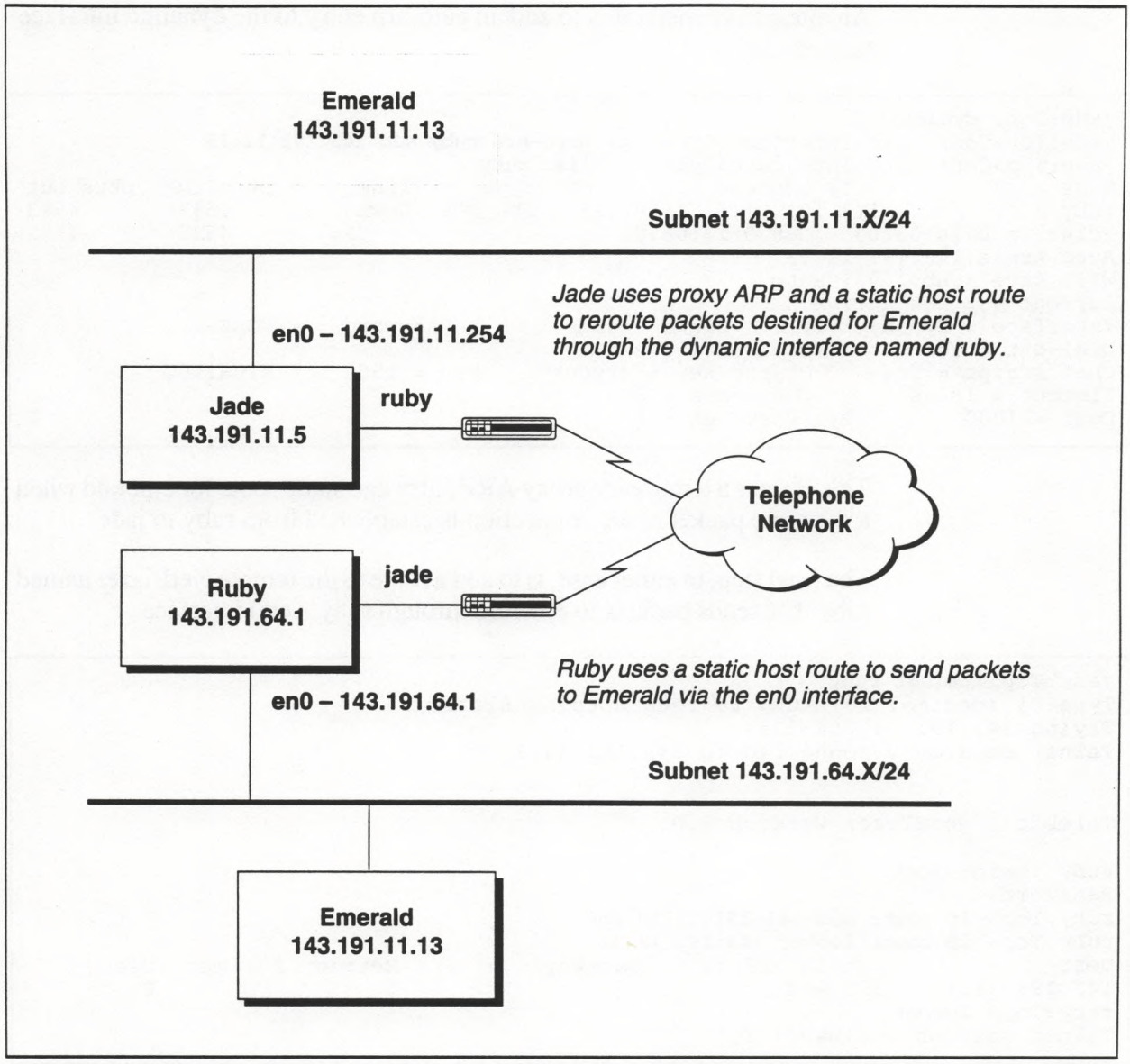


Figure 8-1. Proxy ARP Example

To reroute packets destined for the host named emerald to the remote site, you must add a proxy ARP and static route at the local NetBlazer, jade.

```
jade:Top> arp proxy 143.191.11.13 en0
jade:Top> arp list
received 71 badtype 0 bogus addr 0 reqst in 68 replies 3 reqst out 7
IP addr         Type  Interface   Time Q Addr
143.191.63.255  ether any         0      ff:ff:ff:ff:ff:ff
143.191.11.255  ether any         0      ff:ff:ff:ff:ff:ff
143.191.11.13   ether en0         0      00:80:ad:02:24:9e (published)
jade:Top> route add 143.191.11.13 ruby
adding new route 143.191.11.13 ruby
jade:Top> route lookup 143.191.11.13
Dest            Len Interface    Gateway          Metric  P Timer  Use
143.191.11.13   32  ruby                          1          0      0
```

An alternative method is to add an auto-arp entry to the dynamic interface named ruby.

```
jade:Top> dynamic
jade:Top>Configure>Interface>Dynamic> auto-arp ruby add 143.191.11.13
jade:Top>Configure>Interface>Dynamic> list ruby
Name              IP address   MRU   MTU type     line      pkts in   pkts out
ruby            143.191.11.5  1500  1500 DYN_PPP  Down        4557       4543
Idle: In 0:14:03:03   Out 0:14:03:03                  IP:       4537       4572
Auto Arp's:143.191.11.13
Will save 'ruby' vj: auto
Current vj: not active
Interface = Dynamic PPP     Uname = jade        Password = <<NONE>>
Dial-out = Yes        Dial-in = Yes
Chat script = ics     Crypto key = cryout     MRU = 1500     MTU=1500
Timeout = 180 s       Queue-max = 8
Cost = 1000        Bytespertick = 6
```

This creates a temporary proxy ARP entry and static route for emerald when a dynamic packet mode connection is established from ruby to jade.

The final step, in either case, is to add a route to the remote NetBlazer named ruby that sends packets to emerald through ruby's en0 interface.

```
jade:Top> telnet ruby
Type ^] (decimal 29) <CR> to return to NetBlazer
Trying 143.191.64.254:23...
Telnet session 0 connected to 143.191.64.1


Telebit's NetBlazer Version 2.0

ruby login: root
Password:
ruby:Top> ip route add 143.191.11.13 en0
ruby:Top> ip route lookup 143.191.11.13
Dest            Len Interface    Gateway          Metric  P Timer  Use
143.191.11.13   32  en0                           1          0      0
ruby:Top> logout
Telnet session 0 closed: EOF
```

IP Packet Filtering 9

The **ip filter** commands maintain a list of IP packet filters that are used to restrict IP packet routing to and from designated networks or host addresses through a particular interface.

Input and/or output filtering for a specified interface can be performed on a source address, a destination address, or a source-destination address pair. You can further restrict the filter to only apply to a specified protocol and port number or range.

Initially the packet filter list is empty, which allows all IP packets to pass through the NetBlazer unimpeded. However, adding a filter to the list automatically turns on packet filtering for the specified interface, and all packets routed through that interface are checked for permission to continue.

When packet filtering is turned on for a particular interface, a default filter for that interface is automatically created to be the complement of the first filter. If the first filter is a permit filter, the default filter is set to be a deny filter. On the other hand, if the first filter is a deny filter, the default filter is set to be a permit filter.

Note: *If an interface is assigned filters in only one direction (i.e. all inbound or all outbound filters), the default filter for that interface only applies to packets traveling in the same direction. Packets going in the opposite direction are automatically permitted.*

To determine whether or not an IP packet is allowed to pass through the NetBlazer, it first checks the input interface filter list for an inbound filter that applies to the packet. If the packet is permitted to continue based on a matching inbound filter, the NetBlazer then checks the routing table to verify that a route exists for the packet. If a route exists, the NetBlazer checks the output interface filter list for an outbound filter that applies to the packet. If the packet is also permitted to continue based on a matching outbound filter, it is allowed to pass through the NetBlazer toward its destination.

If the NetBlazer determines that it does not have permission or the ability to route the packet, it discards the packet and sends an ICMP Destination Unreachable message back to the source address of the packet.

To illustrate how IP packet filtering may be used, consider the network shown in Figure 9-1.

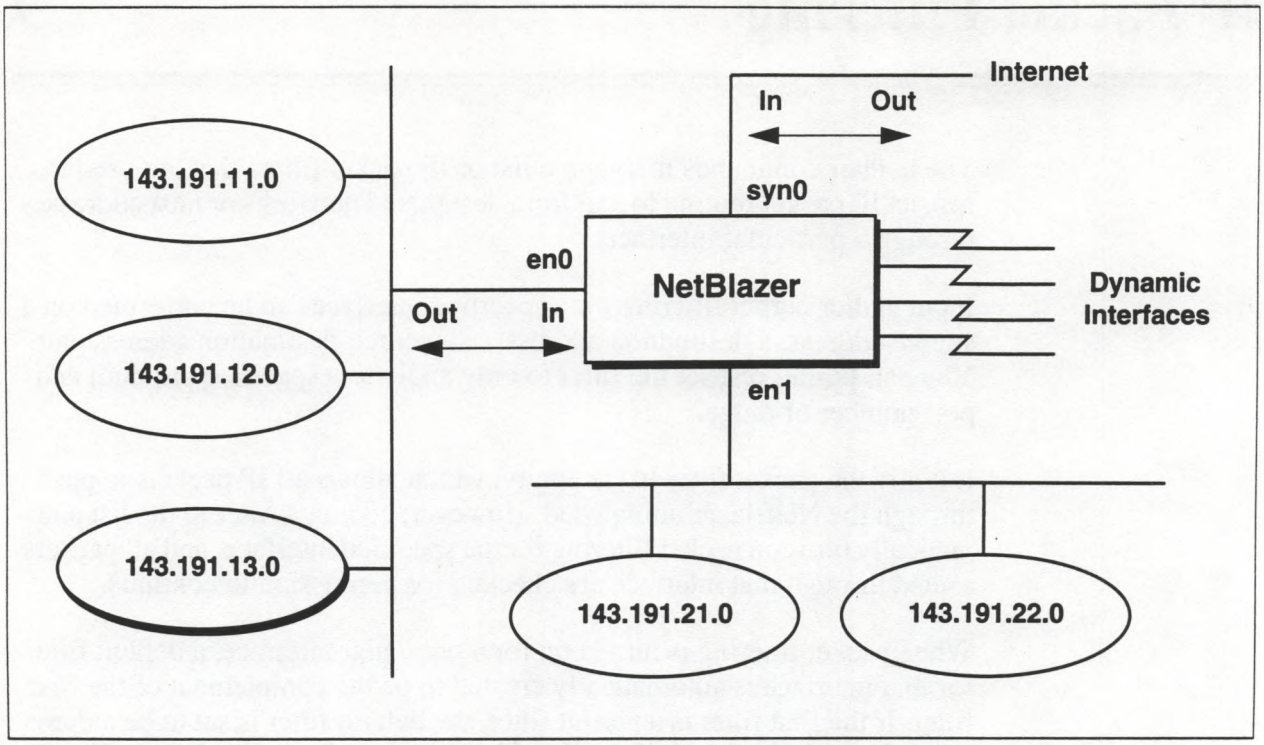


Figure 9-1. Filtering Example Network

Filtering Network IP Addresses

Assuming that you want to allow hosts on the Internet to use the NetBlazer only to reach hosts on the 143.191.0.0 network, go to the Filter command level and add a permit filter for network address 143.191.0.0 via the syn0 interface as shown below.

```
NB:Top> filter
NB:Top>Configure>IP>Filter> permit 143.191/16 syn0
NB:Top>Configure>IP>Filter> list
Source              Destination         Interface Protocol I/O  Permit/Deny
143.191.0.0/16                          syn0               In   Permit
                    143.191.0.0/16      syn0               In   Permit
143.191.0.0/16                          syn0               Out  Permit
                    143.191.0.0/16      syn0               Out  Permit
Default                                 syn0                    Deny
```

At this point, only IP packets with a source or destination address of 143.191.X.X are allowed to pass through the syn0 interface.

Notice that a default filter has been automatically created that denies packets not sent to or from the 143.191.0.0 network from passing through the syn0 interface.This prevents hosts on the Internet from using the NetBlazer to reach a host that is not part of the 143.191.0.0 network.

A more precise way to accomplish the goal from the previous example is illustrated below.

```
NB:Top>Configure>IP>Filter> flush syn0
NB:Top>Configure>IP>Filter> permit 143.191/16 syn0 source out
NB:Top>Configure>IP>Filter> permit 143.191/16 syn0 dest in
NB:Top>Configure>IP>Filter> list
Source              Destination         Interface Protocol I/O  Permit/Deny
                    143.191.0.0/16      syn0               In   Permit
143.191.0.0/16                          syn0               Out  Permit
Default                                 syn0                    Deny
```

The first command in this example removes all filters assigned to the syn0 interface from the list of filters. The next two commands permit outbound packets with a source address of 143.191.X.X or inbound packets with a destination address of 143.191.X.X to pass through the syn0 interface.

Using Filter Lookup to Check a Filter

You can use the **filter lookup** command to confirm that the filters and routing table are set up correctly. For example, to verify that packets can be routed to or from the 143.191.13.0 subnetwork, enter the following commands.

```
NB:Top>Configure>IP>Filter> lookup 128.10.2.1 143.191.13.1 syn0
permission to route the packet granted by syn0 input filters
route to 143.191.13.1 using interface en0
NB:Top>Configure>IP>Filter> lookup 143.191.13.1 128.10.2.1 en0
route to 128.10.2.1 using interface syn0
permission to route the packet granted by syn0 output filters
```

Notice that the <interface> parameter used in the **filter lookup** command must specify the name of the input interface. Otherwise you will get misleading results as shown below.

```
NB:Top>Configure>IP>Filter> lookup 143.191.13.1 128.10.2.1 syn0
permission to route the packet denied by syn0 input filters
```

This example also confirms that an inbound packet destined for a network other than 143.191.0.0 will not be permitted through the syn0 interface.

Filtering Destination Port Numbers

To illustrate how destination port number ranges are used, assume that you want to block outside access to the 143.191.13.0 subnetwork for any purpose other than transferring mail, but you want to allow hosts on this subnetwork to initiate Telnet or FTP sessions.

To accomplish this goal, you should first create deny filters that prevent any packet sent to or from subnetwork 143.191.13.0 from passing through the en0 interface. Then create permit filters that specifically allow packets with the following well-known TCP destination port numbers to pass through the en0 interface from the 143.191.13.0 subnetwork:

Number	Keyword	Description
20	FTP-DATA	File Transfer (Default Data)
21	FTP	File Transfer (Control)
23	TELNET	Terminal Connection
25	SMTP	Simple Mail Transfer Protocol

Port numbers greater than 1023 are generally assigned to server clients at the source when a session is initiated. This assigned port number is used by the server at the other end to send information back to the appropriate client. Therefore, it is important to include a port number range of >1023 in the permit filters to ensure that server responses can be sent back to the client.

The two **filter deny** commands in the next example prevent a packet sent to or from the 143.191.13.0 subnetwork from passing through the en0 interface unless the packet meets the TCP port matching criteria defined by the two **filter permit** commands.

```
NB:Top>Configure>IP>Filter> deny 143.191.13/24 en0 dest out
NB:Top>Configure>IP>Filter> deny 143.191.13/24 en0 source in
NB:Top>Configure>IP>Filter> permit 143.191.13/24 en0 tcp 25 >1023 dest out
NB:Top>Configure>IP>Filter> permit 143.191.13/24 en0 tcp 20-25 !=22 !=24
>1023 source in
NB:Top>Configure>IP>Filter> list en0
Source              Destination         Interface Protocol I/O  Permit/Deny
143.191.13.0/24                         en0       TCP      In   Permit
                                          port rules:  20<= <=25  !=22 !=24
>1023
143.191.13.0/24                         en0                In   Deny
                    143.191.13.0/24     en0       TCP      Out  Permit
                                          port rules: =25 >1023
                    143.191.13.0/24     en0                Out  Deny
Default                                 en0                     Permit
```

Packets destined for subnetwork 143.191.13.0 with a port number equal to 25 or greater than 1023 are allowed to pass through the en0 interface by the first **filter permit** command. Packets sent from the 143.191.13.0 subnetwork with a port number that is equal to 20, 21, 23 or 25 or is greater than 1023 are also permitted to continue through the en0 interface based on the second **filter permit** command.

Caution: *Many servers have assigned port numbers greater than 1023. If you set up permit filters in both directions for port numbers greater than 1023 as in the above example, and do not want outside hosts to reach a server with an assigned port number greater than 1023, you must exclude the port number in the destination permit filter.*

The following example shows you how to exclude destination port 6000 in the 143.191.13/24 en0 destination out permit filter.

```
NB:Top>Configure>IP>Filter> permit 143.191.13/24 en0 tcp !=6000 dest out
NB:Top>Configure>IP>Filter> list en0
Source              Destination         Interface Protocol I/O  Permit/Deny
143.191.13.0/24                         en0       TCP      In   Permit
                                          port rules:  20<= <=25  !=22 !=24
>1023
143.191.13.0/24                         en0                In   Deny
                    143.191.13.0/24     en0       TCP      Out  Permit
                                          port rules: =25 >1023 !=6000
                    143.191.13.0/24     en0                Out  Deny
Default                                 en0                     Permit
```

The above filter list for the en0 interface does not allow UDP or ICMP packets to be sent to or from the 143.191.13.0 subnetwork. Permit filters for each of these protocols must be defined separately. For example, to allow ICMP packets to be sent to or from the 143.191.13.0 subnetwork, enter the following **filter permit** commands.

```
NB:Top>Configure>IP>Filter> permit 143.191.13/24 en0 icmp dest out
NB:Top>Configure>IP>Filter> permit 143.191.13/24 en0 icmp source in
NB:Top>Configure>IP>Filter> list en0
Source              Destination         Interface Protocol I/O  Permit/Deny
143.191.13.0/24                         en0       ICMP     In   Permit
143.191.13.0/24                         en0       TCP      In   Permit
                                          port rules:  20<= <=25  !=22 !=24
>1023
143.191.13.0/24                         en0                In   Deny
                    143.191.13.0/24     en0       ICMP     Out  Permit
                    143.191.13.0/24     en0       TCP      Out  Permit
                                          port rules: =25 >1023
                    143.191.13.0/24     en0                Out  Deny
Default                                 en0                     Permit
```

Note: *ICMP Destination Unreachable messages are sent even if ICMP outbound packets are denied.*

The next series of examples show you how to verify that the filter list is set up correctly.

First, issue a **filter lookup** command to verify that the NetBlazer will still route packets through the en0 interface from a subnetwork other than 143.191.13.0.

```
NB:Top>Configure>IP>Filter> lookup 143.191.12.1 128.10.2.1 en0
permission to route the packet granted by en0 input filters
route to 128.10.2.1 using interface syn0
permission to route the packet granted by syn0 output filters
```

Verify that hosts on the 143.191.13.0 subnet can send packets to Telnet's well-known port number 23 through the en0 interface, and that Telnet (and other servers) have a response path to the 143.191.13.0 subnetwork.

```
NB:Top>Configure>IP>Filter> lookup 143.191.13.1 128.10.2.1 en0 tcp 23
permission to route the packet granted by en0 input filters
route to 128.10.2.1 using interface syn0
permission to route the packet granted by syn0 output filters
NB:Top>Configure>IP>Filter> lookup 128.10.2.1 143.191.13.1 syn0 tcp 1024
permission to route the packet granted by syn0 input filters
route to 143.191.13.1 using interface en0
permission to route the packet granted by en0 output filters
```

Verify that outside hosts cannot telnet into the 143.191.13.0 subnetwork.

```
NB:Top>Configure>IP>Filter> lookup 128.10.2.1 143.191.13.1 syn0 tcp 23
permission to route the packet granted by syn0 input filters
route to 143.191.13.1 using interface en0
permission to route the packet denied by en0 output filters
```

Finally, verify that ICMP messages can be sent to or from the 143.191.13.0 subnetwork.

```
NB:Top>Configure>IP>Filter> lookup 143.191.13.1 128.10.2.1 en0 icmp
permission to route the packet granted by en0 input filters
route to 128.10.2.1 using interface syn0
permission to route the packet granted by syn0 output filters
NB:Top>Configure>IP>Filter> lookup 128.10.2.1 143.191.13.1 syn0 icmp
permission to route the packet granted by syn0 input filters
route to 143.191.13.1 using interface en0
permission to route the packet granted by en0 output filters
```

Filtering Source and Destination Address Pairs

To illustrate how source and destination address pairs are used, assume that you want to prevent hosts on network 128.128.0.0 from communicating with hosts on the 143.191.0.0 network for any purpose other than exchanging mail. This can be accomplished by entering the following commands.

```
NB:Top>Configure>IP>Filter> deny 128.128/16 143.191/16 syn0 tcp <1024 !=25 in
NB:Top>Configure>IP>Filter> deny 143.191/16 128.128/16 syn0 tcp <1024 !=25 out
NB:Top>Configure>IP>Filter> list syn0
Source              Destination         Interface Protocol I/O  Permit/Deny
128.128.0.0/16      143.191.0.0/16      syn0      TCP      In   Deny
                                          port rules: !=25 <1024
                    143.191.0.0/16      syn0               In   Permit
143.191.0.0/16      128.128.0.0/16      syn0      TCP      Out  Deny
                                          port rules: !=25 <1024
143.191.0.0/16                          syn0               Out  Permit
Default                                 syn0                    Deny
```

The two **deny** commands in the above example prevent any packet with a destination port less than 1024 and not equal to the SMTP well-known port 25 from traveling between the 143.191.0.0 and 128.128.0.0 networks through the syn0 interface.

Packets with a TCP destination port equal to 25 or greater than 1023 are permitted through the syn0 interface by the filters assigned to the syn0 interface in a previous example.

Verify that only packets with the SMTP well-known destination port 25 are allowed to pass between the 143.191.0.0 and 128.128.0.0 networks through the syn0 interface by issuing the following **filter lookup** commands.

```
NB:Top>Configure>IP>Filter> lookup 128.128.1.1 143.191.12.1 syn0 tcp 25
permission to route the packet granted by syn0 input filters
route to 143.191.12.1 using interface en0
permission to route the packet granted by en0 output filters
NB:Top>Configure>IP>Filter> lookup 128.128.1.1 143.191.12.1 syn0 tcp 23
permission to route the packet denied by syn0 input filters
NB:Top>Configure>IP>Filter> lookup 143.191.12.1 128.128.1.1 en0 tcp 25
permission to route the packet granted by en0 input filters
route to 128.128.1.1 using interface syn0
permission to route the packet granted by syn0 output filters
NB:Top>Configure>IP>Filter> lookup 143.191.12.1 128.128.1.1 en0 tcp 23
permission to route the packet granted by en0 input filters
route to 128.128.1.1 using interface syn0
permission to route the packet denied by syn0 output filters
```

Deleting a Filter

To illustrate how the **filter delete** command is used, assume that you no longer wish to restrict communications between the 143.191.0.0 and 128.128.0.0 networks. The following example shows you how to remove the filters associated with this restriction.

```
NB:Top>Configure>IP>Filter> list syn0
Source              Destination         Interface Protocol I/O  Permit/Deny
128.128.0.0/16      143.191.0.0/16      syn0      TCP      In   Permit
                                          port rules: =25
128.128.0.0/16      143.191.0.0/16      syn0               In   Deny
                    143.191.0.0/16      syn0               In   Permit
143.191.0.0/16      128.128.0.0/16      syn0      TCP      Out  Permit
                                          port rules: =25
143.191.0.0/16      128.128.0.0/16      syn0               Out  Deny
143.191.0.0/16                          syn0               Out  Permit
Default                                 syn0                    Deny
NB:Top>Configure>IP>Filter> delete 128.128/16 143.191/16 syn0
NB:Top>Configure>IP>Filter> delete 128.128/16 143.191/16 syn0 tcp
NB:Top>Configure>IP>Filter> delete 143.191/16 128.128/16 syn0
NB:Top>Configure>IP>Filter> delete 143.191/16 128.128/16 syn0 tcp
NB:Top>Configure>IP>Filter> list syn0
Source              Destination         Interface Protocol I/O  Permit/Deny
                    143.191.0.0/16      syn0               In   Permit
143.191.0.0/16                          syn0               Out  Permit
Default                                 syn0                    Deny
```

Modem Server Configuration 10

Using the NetBlazer as a modem server allows users on the IP network to telnet to the NetBlazer and establish a serial character mode connection with a remote system.

This chapter includes the following four sections:

- **Setting Up Dial-Out Destination Records** – shows you how to set up one or more dial-out records used to call a remote site.
- **Using Characteristics Groups** – explains how to use the characteristics group function to select a line and preconfigure the modem for a dial-out connection.
- **Setting Up a Modem Pool** – describes how to configure the NetBlazer to allow users to telnet to a modem from an IP host on the network and call a remote system using the modem's dial command.
- **Allowing Direct Number Dialing** – describes how to configure the NetBlazer to allow users to dial a telephone number directly without requiring a dial-out record.

Setting Up Dial-Out Destination Records

The NetBlazer dial-out records include the following information, which is used to establish a connection with the remote system:

- **Dialout Name** – This is the name assigned to the dial-out record. It is used by other routines in the NetBlazer to select the dial-out record that contains the information needed to call the remote site.
- **Phone Number** – This is the telephone number used to call the remote system.
- **Characteristics Group** – This is the name of the characteristics group that is assigned to the dial-out record. Information contained in the characteristics group record is used to select and preconfigure a modem for calling the remote system.
- **Character Mode Timeout** – This field determines how long a character mode connection is allowed to be idle before disconnecting the call. Packet mode connections use a different timeout, which is set in the dynamic interface record.
- **Minwait and Maxwait** – These two fields determine the minimum and maximum number of seconds that the NetBlazer must wait before it can use the dial-out record to place another call.

- **Username, Password, and/or Crypto Key** – These fields include the login information used to authenticate a dial-out connection with a remote system.
- **Chat Script** – This field identifies which script in the CHAT.TXT file to use during an authentication dialog with the remote system. For NetBlazer-to-NetBlazer packet mode connections, use the ics chat script. For NetBlazer-to-NetBlazer character mode connections initiated through the **session chatdial** command, use the login chat script.

Adding a Dial-Out Destination

To add an entry to the dial-out destination list, enter an **add** command at the Configure Dialout command level.

```
jade:Top> dialout
jade:Top>Configure>Dialout> add
```

The NetBlazer prompts you for the required information:

```
Name of dialout: gemini
```

The destination name entered is used by other routines in the NetBlazer to select this record. If the destination is another NetBlazer with more than one modem connected, enter the same destination name for each telephone line connected to the remote NetBlazer.

```
Phone number: 9-555-1234
```

Enter the telephone number of the remote connection. Refer to the Dial command description in your modem's reference manual for a description of acceptable dial strings.

```
Line characteristics (dialout):
```

This entry is used to select a serial line with matching characteristics when placing a call to the dial-out destination. If no line is available with the specified characteristics, the call is not made. The name entered must be an existing characteristics group. Press the return key to accept the default characteristics group, dialout.

```
Char mode timeout (in minutes) [60]:
```

This entry sets the number of minutes that the NetBlazer maintains an idle character mode connection. Enter the number of minutes or press return to accept the default value of 60 minutes.

```
Dialout: name=gemini, phone=9-555-1234, characteristics=dialout
Okay (yes|no|quit) [y]?
```

If the dial-out record that you just entered is correct, press the return key or enter **y** to accept the record. If you want to discard this record and enter a new record, enter **n** at the prompt. If you want to discard this record and return to the NetBlazer's command prompt, enter **q** to quit.

The dial-out destination can be reached through a **session dial** command or through a **session connect** command if the destination is included in the user's destination group as described in Chapter 11, User IDs and Destination Groups.

For information on listing and changing a dial-out record's parameters, refer to Dialout Commands in the *NetBlazer Command Reference Manual.*

Using Chat to Automatically Log In to a Remote System

To set up a dial-out record to automatically log in to a remote system, you can assign a chat script, user name, and password or crypto key to a dial-out record, as illustrated below.

```
jade:Top>Configure>Dialout> chat gemini login
jade:Top>Configure>Dialout> uname gemini jade
jade:Top>Configure>Dialout> password gemini passport
```

This allows NetBlazer users to establish a character mode connection and automatically log in to the remote system, gemini, by issuing a **session chatdial gemini** command.

The **dialout chat** <dialout> <chat-script-name> command assigns a chat script to the dial-out record. The chat script must exist in the CHAT.TXT file. You can create custom chat scripts by editing the CHAT.TXT file, as described in Appendix A, NetBlazer File Definitions.

The **dialout uname** <dialout> <remote-username> command sets the user name that is sent to the remote system by the NetBlazer's chat routine. Likewise, the **dialout password** <dialout> <remote-password> command sets the password sent to the remote system. The remote system should include a matching user name and password in its user records to authenticate the connection.

Using Characteristics Groups

The NetBlazer uses the characteristic group records assigned to the lines and dial-out records along with information contained in the MODEMCAP.TXT file to select and preconfigure a modem before calling a remote site.

Preconfiguring a Modem for a Dial-Out Destination

Each characteristics group record contains one or more user-defined tags. The NetBlazer selects a line and preconfigures the modem by matching the user-defined tags in the characteristics group that is assigned to a dial-out record with the characteristic tags contained in the line's characteristic group or in the MODEMCAP.TXT file.

Displaying a list of the characteristics groups shows seven groups that are provided by Telebit.

```
jade:Top>Configure>Dialout> group
jade:Top>Configure>Group> list
dialout
v32dialout
request
pepdialout
raw
raw_dial
v25dialout
```

The dialout group is the default group, which is assigned to each line with a modem attached when the Netblazer is first powered up. Listing the dialout group shows that this group has one characteristic tag; i.e., dialout.

```
jade:Top>Configure>Group> list dialout
Group :
    dialout
Characteristics :
    0: dialout
```

Assigning the dialout characteristic group to a dial-out record allows the NetBlazer to use any line that has a dialout characteristic group assigned to it when placing a call to the destination specified by the dial-out record. This also allows the modem to use its default configuration, which is defined by the MODEMCAP.TXT file.

Using the default modem configuration is preferred in most cases because it allows the modem to negotiate the operating mode with the modem at the remote site.

However, suppose that you want to force the modem to always use the V.32 transmission mode when calling a particular dial-out destination. Listing the v32dialout characteristic group shows that this group has two characteristic tags assigned to it.

```
jade:Top>Configure>Group> list v32dialout
Group :
    v32dialout
Characteristics :
    0: dialout
    1: v32
```

The v32 characteristic tag is a special tag defined in the MODEMCAP.TXT file. When the NetBlazer detects this tag while using a dial-out record to place a call, it selects a modem that supports V.32 mode and preconfigures the modem for V.32 modulation.

The following example shows you how change the characteristic group assigned to an existing dial-out record named gemini.

```
jade:Top>Configure>Group> dialout
jade:Top>Configure>Dialout> characteristics gemini v32dialout
jade:Top>Configure>Dialout> list
Name              Phone               Characteristics
tbupdate          1-408-745-3700      dialout
gemini            9-555-1234          v32dialout
```

Listing the dial-out records show that the v32dialout characteristic group is assigned to the dial-out record for gemini.

Figure 10-1 illustrates how the NetBlazer uses the v32dialout characteristics group to select and preconfigure the modem for V.32 transmission mode by matching the characteristic tags contained in the dialout characteristics group to the characteristic tags contained in the line characteristics group and MODEMCAP.TXT file.

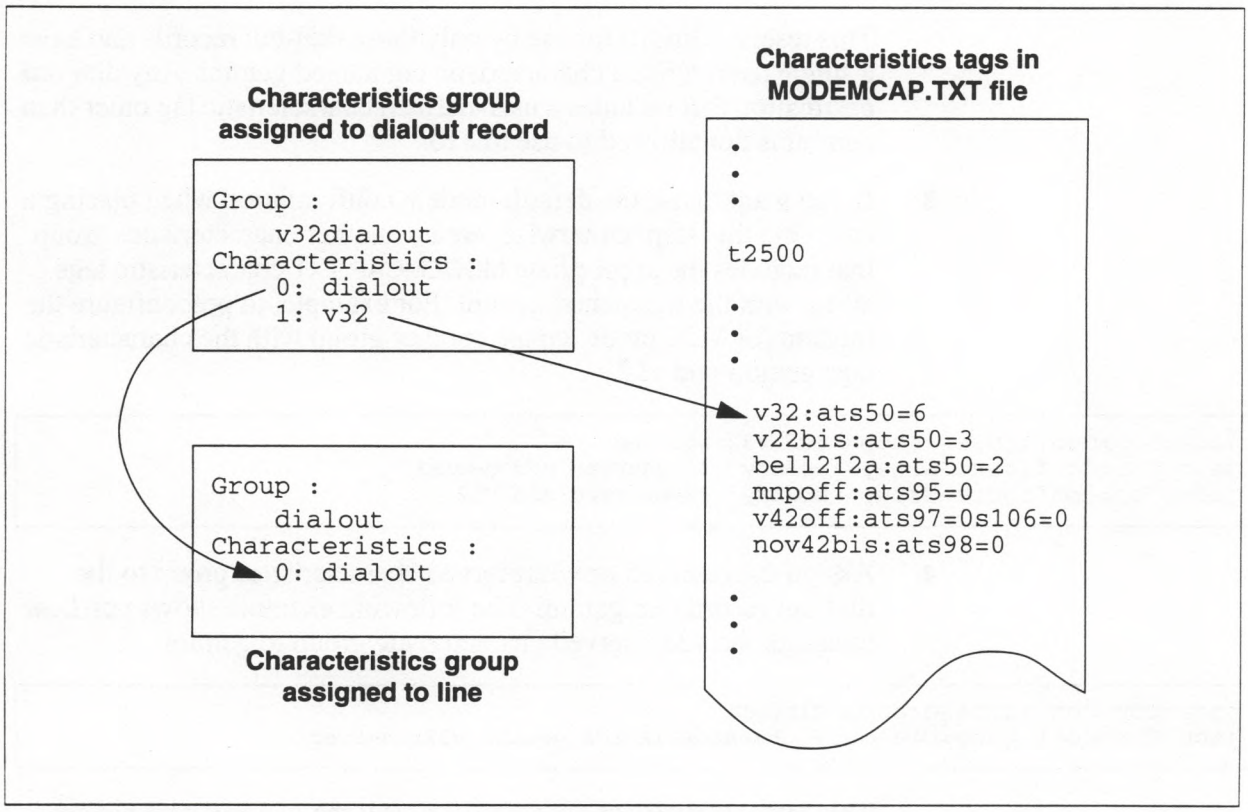


Figure 10-1. Using Characteristic Tags to Preconfigure the Modem

Before placing a call to the destination named gemini, the NetBlazer selects a line that has a dialout characteristic tag in its assigned characteristics group and has a modem attached that supports V.32 transmission mode. It then sends the v32 command string, defined in the MODEMCAP.TXT file, to the modem.

Restricting the Use of a Line for Specific Dial-Out Destinations

You can create custom line characteristics groups to restrict the use of one or more serial lines for a select group of dial-out destinations. For example, to reserve line10 exclusively for use by the dial-out destination named gemini, perform the following steps:

1. Go to the Configure Group command level and create a new group, named reserved, with a characteristic tag named gemini.

```
jade:Top>Configure>Dialout> group
jade:Top>Configure>Group> add reserved
jade:Top>Configure>Group> modify reserved add gemini
```

2. Assign the reserved characteristics group to line10.

```
jade:Top>Configure>Group> line characteristics line10 reserved
```

This reserves line10 for use by only those dial-out records that have a single user-defined characteristic tag named gemini. Any dial-out destination that includes a user-defined characteristic tag other than gemini is not allowed to use line10.

3. If you want to use the default modem configuration when placing a call, skip this step. Otherwise, create another characteristics group that includes the appropriate MODEMCAP.TXT characteristic tags along with the tag named gemini. For example, to preconfigure the modem for V.32 mode, create another group with the characteristic tags gemini and v32.

```
jade:Top>Configure>Group> add v32reserved
jade:Top>Configure>Group> modify v32reserved add gemini
jade:Top>Configure>Group> modify v32reserved add v32
```

4. Assign the reserved or v32reserved characteristics group to the dial-out records for gemini. The following example shows you how to assign the v32reserved characteristic group to gemini.

```
jade:Top>Configure>Group> dialout
jade:Top>Configure>Dialout> characteristics gemini v32reserved
```

This lets the NetBlazer use line10 to call the dial-out destination named gemini in V.32 mode. If you want the dial-out record to use the modem's default configuration, enter reserved in place of v32reserved in the above example.

If your site has many users that need to dial out to many different sites, you can configure the NetBlazer to allow IP users to telnet from a host on the network to a pool of modems and then use the modem's dial command to call a remote system.

To set up a modem pool, you must create a special characteristic group and assign an IP address to the group.

```
jade:Top> group
jade:Top>Configure>Group> add pool
jade:Top>Configure>Group> modify pool add dialout
jade:Top>Configure>Group> modify pool add sane
jade:Top>Configure>Group> ip address 143.191.11.10 pool 23
jade:Top>Configure>Group> list pool
Group :
    pool
Characteristics :
    0: dialout
    1: sane
Modem pooling Telnet IP address: 143.191.11.10
```

As shown in the above listing, the characteristics group named pool includes two characteristic tags – dialout and sane. The sane characteristic tag is a special tag defined in the MODEMCAP.TXT file that puts the modem into a human-friendly mode.

Assigning an IP address to a characteristics group allows IP users on the network to talk to the first available modem that meets the requirements of the characteristic group.

```
napa > telnet 143.191.11.10
Trying 143.191.11.10 ...
Connected to 143.191.11.10.
Escape character is '^]'.
Connected to modem pool line "line10"
AT
OK
```

When a connection with the modem is established, the IP network user can use the modem's dial command (e.g., **atdt** <phone-number>) to dial out to a remote system.

When the user terminates the telephone connection with the remote system, the connection between the network host and the modem is closed.

Entering a **security numberdial enable** command allows all users to dial phone numbers directly using the **session dial** <phone-number> command.

```
jade:Top> security
jade:Top>Configure>Security> numberdial enable
jade:Top>Configure>Security> numberdial
Anyone may dial phone numbers directly
```

This lets users log in to the NetBlazer and call a remote system without requiring a dial-out record for the remote site.

User IDs and Destination Groups 11

Every user who logs in to the NetBlazer, either through a telnet session or by calling in from a remote terminal, must have an assigned user ID record. User records are saved in a PASSWD file, which is located either on the NetBlazer system diskette or on a remote system.

First Decide Where to Keep the NetBlazer User Records

Because the PASSWD file format is similar to the file format of a UNIX password file, sites with a large number of UNIX users have several choices, listed below, as to how to maintain the NetBlazer user list.

- Use the **user add** command to manually add individual users to the local user list.
- Use the **user load** <host>:<pathname> command to download user records from a UNIX password file on a remote UNIX host.
- Use the **files passwd** <host>:<pathname> command in the FILES.CNF file to download user records from a UNIX password file on a remote UNIX host when the NetBlazer is powered up or rebooted.
- Use the **user remote** <host>:<pathname> command to direct the NetBlazer to look in a specified remote password file if the user is not found in the local user list.
- Use the DNS facility on a remote host to maintain a list of NetBlazer users.

You can use any combination of the above options to set up and maintain the list of authorized NetBlazer users. In fact if you decide to use a remote password file, you should set up a small group of local users with system configuration privileges in case the NetBlazer is not able to reach the remote host.

If you want to maintain some or all of your user records in a password file on a remote host, refer to Chapter 14, Network Management, for instructions on how to configure the NetBlazer and the IP host to use a remote password file.

For a description of the NetBlazer's password file format, refer to Appendix A, NetBlazer File Definitions.

Adding Local User Records

This section describes how to manually add a user ID to the NetBlazer's local list of authorized users. Before adding users, consider setting up destination groups for the users. Doing so has the following advantages:

- Simplifies user interaction with the NetBlazer by allowing users to select a telnet or dialout destination from a list of destinations assigned to the users.
- Allows you to restrict the user's access to a limited group of IP hosts and/or dialout destinations.

An alternative to setting up destination groups for users who have only one destination is to assign a login command to the user that automatically connects the user to his or her destination.

See Setting Up User Destination Groups on page 11-4 for instructions on creating destination groups. For instructions on how to automatically connect a user to a predetermined destination see Automatically Connecting a User to a Specific Destination on page 11-7.

To manually add a user to the list of local users, enter a **user add** command.

```
jade:Top> user
jade:Top>Configure>User> add
Enter the uname (1-32 chars): charlie
```

The uname is the name that the user enters to log in to the NetBlazer.

```
What kind of user ([character], SLIP, PPP, ARA, ACS):
```

Press the return key or enter **c** to add a character mode login user to the list.

The NetBlazer uses SLIP and PPP user records to authenticate packet mode connections from remote networks. See Chapter 6, Dynamic IP Interface Configuration, for instructions on how to set up packet mode connections.

ARA user records authenticate ARA connection requests received from remote Macintosh systems. See Chapter 16, AppleTalk Configuration for instructions on how to setup ARA connections.

ACS user records authenticate ACS connection requests received from remote PC systems that are running NetBlazer ACS software. You must have the ACS option installed on the NetBlazer system diskette to set up an ACS user. See the *NetBlazer ACS Reference Manual* for instructions on how to setup ACS connections.

```
Want to enter a password [y]?
```

Press the return key if you want to assign a password to this user. You will be prompted for the password. If you do not want to assign a password to this user enter **n** at the prompt.

```
Enter the password (no echo):
Re-enter the password:
```

Enter the user's password. The password is not displayed on the screen as you type it, so you are asked to enter the password twice to ensure that you entered it correctly.

```
Issue a crypto handshake [n]?
```

Unless this user has some way of responding to a crypto challenge, press the return key or enter **n** to prevent the NetBlazer from issuing a crypto challenge to the user during the login process.

```
Allow system configuration privileges (n/y) [n]?
Allow system status privileges (n/y) [n]?
```

Only the system administrator and designated staff should be granted system configuration or status privileges. If this is one of those users, enter **y** to either of the above prompts.

If you grant system configuration privileges to this user, the NetBlazer will automatically grant status privileges to the user.

```
Allow dialout access (n/y) [y]?
Allow telnet access (n/y) [y]?
```

Answering **n** to either of these prompts limits a user's dialout, telnet/rlogin access to only destinations that are in the user's assigned destination group.

If the user is assigned to a destination group that does not include at least one dialout, telnet or rlogin destination, answering **n** to any of the above prompts blocks the users ability to establish that type of connection. For example, if you do not want to allow a user to dial out from this NetBlazer, answer **n** to the **Allow dialout access** prompt and assign the user to a destination group that does not include a dialout destination.

```
Assign to a destination group (y/n) [n]? y
Enter the destination group name: marketing
```

If you have a destination group for this user, answer **y** to the first prompt, and enter the name of the destination group. Otherwise, press the return key or enter **n** at the first prompt. You can assign a destination group to the user later by issuing a **user destgroup** <userid> <destination> command.

```
User: charlie          privs:     dest-group: marketing
Okay (yes|no|quit) [y]?
```

Press the return key or enter **y** to accept the above user ID record. Otherwise, enter **n** or **q** to discard this record.

Setting Up User Destination Groups

Destination groups allow users to easily establish a connection with a selected destination (IP host or remote computer) by simply specifying the desired destination through the **session connect** command.

To illustrate how destinations groups are used, consider the organization shown in Figure 11-1.

Mike and Connie are sales people, requiring access to the corporate sales computer via a dial-in connection from a remote site. They sometimes also need to get information from the customer service computer. Creating a sales destination group with two destinations, sales and service, and assigning this destination group to Mike's and Connie's user account allows them to dial into the NetBlazer and establish a telnet session with the Sales or Customer Service computer by issuing a **connect sales** or **connect service** command to the NetBlazer.

Brian is a field service representative and only needs access to the Customer Service computer at the corporate office. Creating a service destination group with only one destination, service, should meet Brian's requirements.

Charlie works in Marketing, and has a workstation at both the corporate office and at his home. He needs access to the marketing computer from either location. He also occasionally needs to dial out to the data bank computer for additional information. Creating a marketing destination group with two destinations, a telnet connection with the marketing computer, and a dialout connection with the data bank computer should satisfy Charlie's requirements.

To set up the marketing destination group, used by Charlie, first create a dialout record for the data bank computer as described in Chapter 10.

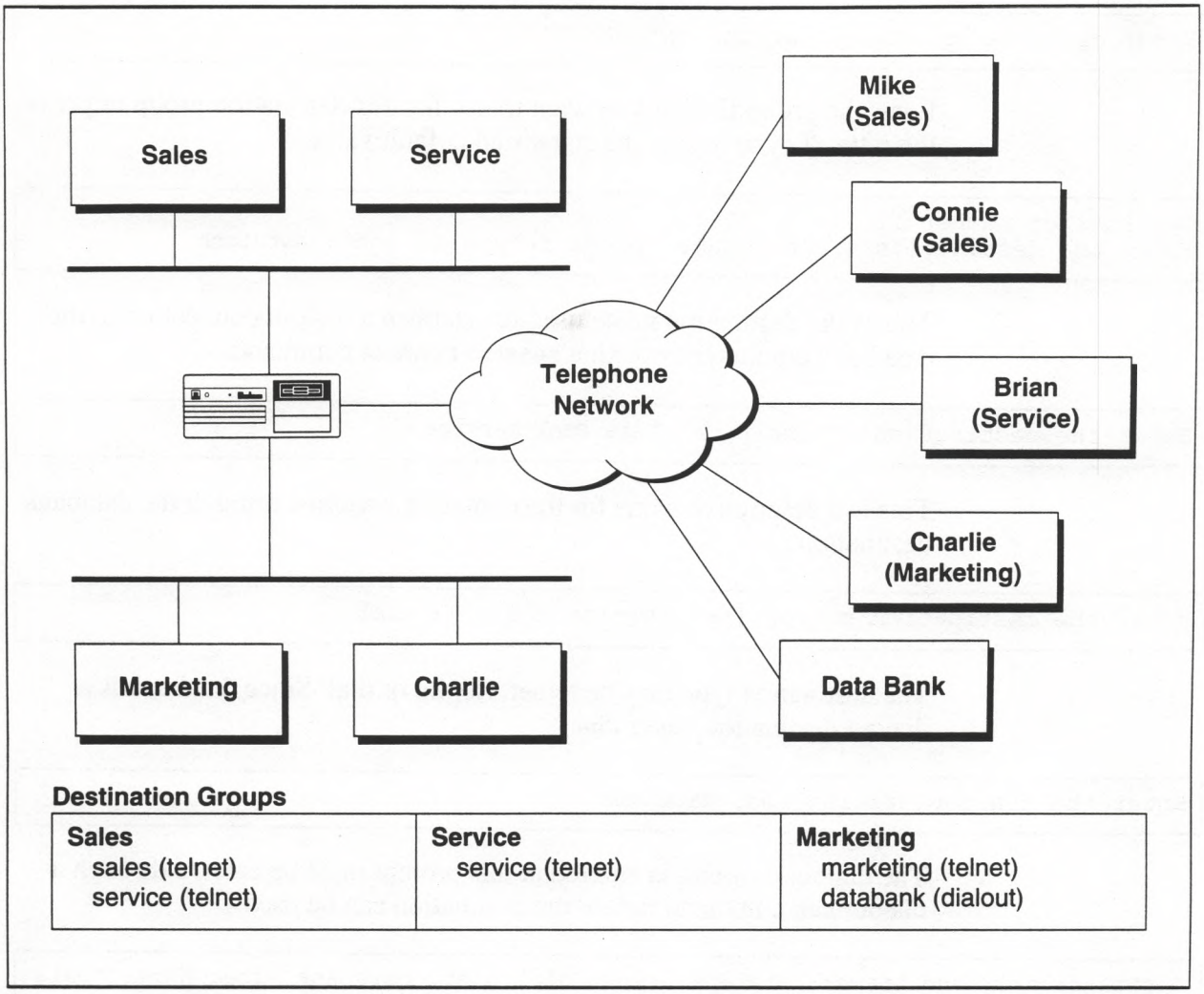


Figure 11-1. Destination Group Example

Next, go to the Configure Destination command level and enter **add** at the command prompt.

```
jade:Top> destination
jade:Top>Configure>Destination> add
```

You are prompted for the required information:

```
Please enter the name of the destination group: marketing
Destination group marketing doesn't exist; creating it.
```

This is the destination group name assigned to Charlie and any other users in the marketing group.

```
Enter group id or <CR> to accept default [1]:
```

Enter the group ID that you want to use for this destination group or press the return key to accept the suggested default value.

```
Destination number 1.
Enter the destination's short name (press return to end): databank
```

This is the destination name used to establish a dialout connection to the data bank computer through a **session connect** command.

```
Enter the destination's long name: Data Bank Service
```

This is a descriptive name for the computer accessed through the databank destination.

```
Enter the destination's type [telnet|rlogin|dial]: dial
```

The destination type may be telnet, rlogin, or dial. Since databank is a dialout destination, enter **dial**.

```
Enter the dialout destination: databank
```

The dialout destination entered at this prompt must be created through a **dialout add** command before the destination can be used.

```
Destination 1: shortname: databank  type: dial host: databank  long name: "Data
Bank Service"
Do you really want to enter this destination (y/n) [y]?
```

This prompt allows you to verify that the destination information is correct, before accepting the entry. Press the return key or enter **y** to accept the entry.

```
Destination number 2.
Enter the destination's short name (press return to end): marketing
```

This is the destination name that is used to connect to the marketing computer through a **session connect** command.

```
Enter the destination's long name: Marketing Computer
```

Information entered in this field is used to further describe the machine that is accessed through this destination.

```
Enter the destination's type [dial]: telnet
```

The destination type may be telnet, rlogin, or dial. Since the marketing computer is connected to the network, this is a telnet or rlogin destination.

```
Enter the telnet hostname: marketing
```

The telnet hostname may be either a domain name or an IP address. To use a domain name, the NetBlazer must be configured to use the domain naming system.

```
Destination 2: shortname: marketing  type: telnet host: marketing  long
name: "Marketing Computer"
Do you really want to enter this destination (y/n) [y]?
```

This prompt allows you to verify that the destination information is correct. Press the return key or enter "y" to accept the entry.

```
Destination number 3.
Enter the destination's short name (press return to end):
```

When you have entered information for all destinations in this destination group, press the return key to quit this dialog and return to the NetBlazer command prompt.

Enter a **list** command at the Top>Configure>Destination> prompt to display a list of the current destination groups.

```
jade:Top>Configure>Destination> list marketing
Gid  Group/#          Short Name      type Host             Long Name
1    marketing
      1              databank          D  databank         "Data Bank Service"
      2              marketing         T  marketing        "Marketing Computer"
```

The above listing shows that the marketing destination group includes two destinations, a telnet destination to marketing and a dialout destination through the databank dialout destination.

This destination group can now be assigned to Charlie and any other user in the marketing group through the **user add** or **user destgroup** commands.

Automatically Connecting a User to a Specific Destination

If you have users that only use the NetBlazer as an intermediary to connect to a single destination, you can assign those users a login command that automatically starts a session with a predetermined destination when the user logs into the NetBlazer. For example, suppose that you have a user

named Carol who uses the NetBlazer to call in from home and telnet to a host system named napa. Set up a user account and login command that automatically connects Carol to napa whenever she logs into the NetBlazer as illustrated below.

```
jade:Top> user
jade:Top>Configure>User> add carol
jade:Top>Configure>User> command carol "telnet napa; logout"
```

The **user command** command in the above example performs two functions. First, it automatically starts a telnet session with the host named napa when Carol logs in to the NetBlazer. Second, it logs Carol out of the NetBlazer when she has completed her session with napa.

Note: *When assigning multiple commands to a user's login command as shown in the above example, be sure to separate the commands with a semicolon and enclose the commands in quotes.*

If you have several users, like Carol, who need to automatically connect to napa from the NetBlazer, consider create a user account for napa that can be used by any user logging into the NetBlazer as napa.

```
jade:Top> user
jade:Top>Configure>User> add napa
jade:Top>Configure>User> command napa "telnet napa; logout"
```

Setting Up Callback Security 12

The NetBlazer can be configured to call back a remote user at a specified destination. When callback security is used, the remote user must call the NetBlazer at the telephone number associated with the callback request line. The NetBlazer prompts the caller for the dialout destination to call back, then disconnects the original call and calls the user back at the user-specified destination.

Setting Up a Callback Request Line

To set up the NetBlazer to use callback security, you need to configure one or more of the asynchronous lines as a callback request line. No one can log in on a line that has been designated for processing callback requests. The following example shows you how to set up line10 as a callback request line.

```
jade:Top> line
jade:Top>Configure>Line> request-call line10 on
Request-callbacks on line 'line10' is on
```

Remote users should use this line to call into the NetBlazer to request a call-back. When a call is received on line10 in the above example, the NetBlazer prompts the caller for a destination. The destination entered must exist in the dial-out list. Therefore, you must create a dial-out record for each site that uses callback security (see Setting Up Dial-Out Destination Records in Chapter 10).

Callback with Auto-Telnet

This section describes how to configure the NetBlazer to automatically establish a telnet session with a predetermined host system when calling back a specified destination site.

First, set up a callback request line as described in the previous section. Then configure one or more lines to automatically telnet to a specific host.

```
jade:Top>Configure>Line> group add napa
jade:Top>Configure>Line> group modify napa add napa
jade:Top>Configure>Line> characteristics line11 napa
jade:Top>Configure>Line> command line11 telnet napa
```

The previous example creates a new characteristics group named napa, then assigns the group to line11 and configures the line to automatically connect with the host system named napa.

Next, turn off the callin parameter for each line that is used to call back a specified destination site, as shown below.

```
jade:Top>Configure>Line> callin line11 off
Callin on line 'line11' is off
```

This prevents a user from calling directly into the host system without going through the callback security process.

Finally, create dial-out records for each site that can be called back from the NetBlazer. The following example shows you how to set up a dial-out record for a remote destination site named saturn.

```
jade :Top>Configure>Line> dialout add saturn 555-8912 napa
```

When a user calls into the NetBlazer on the callback request line and enters "saturn" as the callback destination site, the NetBlazer looks up saturn in its dial-out list, selects a line that matches saturn's characteristics group (i.e., napa), and calls the user back at the telephone number specified for saturn. In this example, the NetBlazer uses line11 to call back saturn. Because this line is configured to automatically telnet to napa, the user is connected directly with napa when the connection is established.

Packet Mode Callback

This section describes how to set up callback security for a packet mode connection between two NetBlazers.

First set up a callback request line on the local NetBlazer, as described on page 12-1. Then use **pppdial**, **slipdial**, or **ipdial** to set up a dynamic interface on both the local and remote NetBlazers. To allow either site to initiate a dial-up connection, configure both NetBlazers to permit dial-in and dial-out connections through their respective interfaces.

When setting up the dynamic interface on the remote NetBlazer, enter the telephone number associated with the callback request line on the local NetBlazer. This allows the remote NetBlazer to request a callback by calling the local NetBlazer's callback request line.

The NetBlazer's default chat script (isc) is set up to send the dial-out record's user name in response to a Where: prompt from the answering NetBlazer. Make sure that the local NetBlazer's interface and dial-out record names match the user name sent by the remote NetBlazer. Also, be sure to use the ics chat script with the remote NetBlazer's interface.

The following two displays show how to set a local NetBlazer named jade to accept a callback request from a remote NetBlazer named ruby for a packet mode connection.

Local NetBlazer (jade) configuration:

```
jade:Top> line
jade:Top>Configure>Line> request-call line10 on
Request-callbacks on line 'line10' is on
jade:Top>Configure>Line> dynamic
jade:Top>Configure>Interface>Dynamic> pppdial
Name of the remote (other) system: ruby
Phone number: 9-555-1234
Authentication method (crypto, password, none) [c]:
Enter the crypto key (no echo):
Re-enter the crypto key:
Add dialout 'ruby'
Add user 'ruby'
Add dynamic interface=ruby, user=jade chat=ics, with crypto handshaking
 using PPP, MRU=1500
Okay (yes|no|quit) [y]?
REMINDER! You need to set up route(s) for this interface
jade:Top>Configure>Interface>Dynamic> ip route add 143.191.64/24 ruby
adding new route 143.191.64/24 ruby
```

Remote NetBlazer (ruby) configuration:

```
ruby:Top> dynamic
ruby:Top>Configure>Interface>Dynamic> pppdial
Name of the remote (other) system: jade
Phone number: 9-555-9876
Authentication method (crypto, password, none) [c]:
Enter the crypto key (no echo):
Re-enter the crypto key:
Add dialout 'jade'
Add user 'jade'
Add dynamic interface=jade, user=ruby chat=ics, with crypto handshaking
 using PPP, MRU=1500
Okay (yes|no|quit) [y]?
REMINDER! You need to set up route(s) for this interface
ruby:Top>Configure>Interface>Dynamic> ip route add 143.191/16 jade
adding new route 143.191/16 jade
```

When the remote NetBlazer (ruby) requires a packet mode connection with the local NetBlazer (jade), it calls jade's callback request line and sends the user name ruby in responses to the "Where:" prompt from jade. Jade then disconnects the call and uses the dial-out record for ruby to call back and establish a packet connection with ruby.

Setting Up a Raw TCP Link 13

The raw server allows you to establish a raw TCP connection from a host on the network to the modem or other asynchronous device attached to a NetBlazer line. Raw data from the host is transferred directly to the device attached to the line that has been set up for a raw connection. Data from a raw connection is encapsulated in TCP/IP packets and sent back to the host on the network.

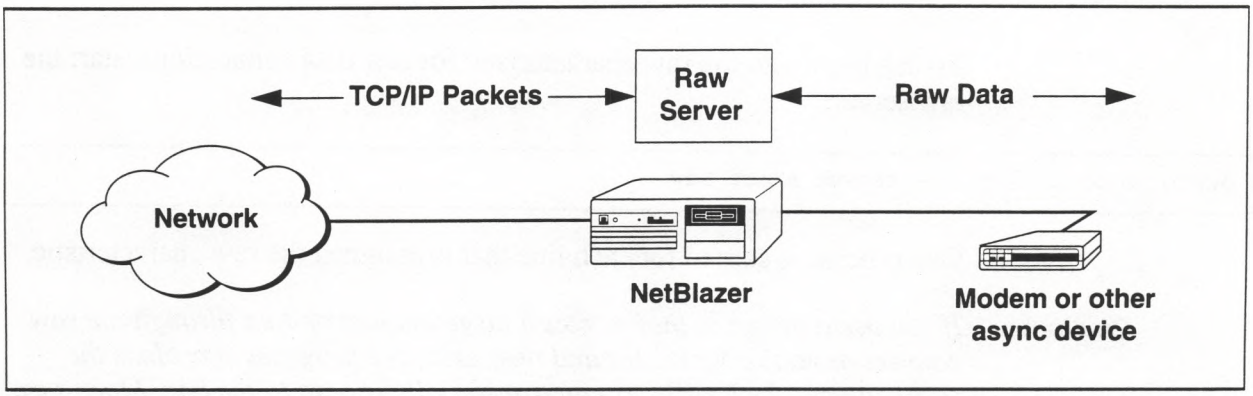


Figure 13-1. Raw TCP Connection

Configuring a Line for a Raw Connection

To configure a line for a raw connection, assign the line a characteristic group that includes the raw characteristic tag. Two characteristic groups provided by Telebit include the raw characteristic tag: raw and raw_dial. The raw characteristic group allows only raw connections on the line. The raw_dial characteristic group allows both raw connections and dial-out connections if a modem is attached to the line.

Assigning a Characteristic Group

Go to the Configure Line command level and assign the raw or raw_dial characteristic group to the line that you want to use for a raw connection.

```
pearl:Top> line
pearl:Top>Configure>Line> characteristic line01 raw_dial
```

Assigning a characteristic group to a line with the raw characteristic tag automatically assigns an IP address and port number to the line unless they are already set. The defaults are the NetBlazer's global IP address and a port number equal to 7000 plus the line number (for example, line01 is assigned port number 7001).

Changing the Line's IP Address

Using the NetBlazer's global IP address the default port number assigned to the line is preferred. However if you must change a line's IP address or port number, use the **ip address** <ip-addr> <linename> [<port>] command, as shown in the following example:

```
pearl:Top>Configure> ip address 143.191.10.28 line01 543
```

Starting the Raw Server

To use lines with the raw characteristic for raw data connections, start the raw server.

```
pearl:Top>Configure> server start raw
```

One process is started for each line that is assigned the raw characteristic.

Caution: *If you use a program that pushes a large amount of data through the raw connection to the NetBlazer and then exits, the program may close the socket before the NetBlazer can transfer all the data to the line. Make sure such programs wait a sufficient amount of time to let the NetBlazer drain the socket.*

Stopping a Raw Connection

To stop all raw services, enter a **server stop raw** command.

```
pearl:Top>Configure> server stop raw
```

To stop the raw service on an individual line, assign the line to a characteristic group that does not contain the raw characteristic tag.

```
pearl:Top> line
pearl:Top>Configure>Line> characteristic line01 dialout
```

This automatically stops the raw server listening for that line.

Stopping the raw server in either way does not stop raw sessions in progress. To interrupt a raw session in progress, use the **line reset** command for the line you wish to stop.

Network Management 14

This chapter provides instructions on how to remotely boot and manage the NetBlazer over a TCP/IP network.

Booting the NetBlazer from a UNIX Host

You can configure the NetBlazer to boot over a TCP/IP network the same way that a diskless workstation boots from a file server on the network. This lets you to keep a single copy of the NetBlazer software and configuration files at a central location.

The NetBlazer uses BOOTP and TFTP client services to boot from a UNIX host that is connected to the same Ethernet segment as the NetBlazer's en0 interface. To allow machines to reach a BOOTP server located on the other side of a NetBlazer, the NetBlazer includes a BOOTP forwarding server. This service is provided primarily to support sites with multiple NetBlazers, but it also should work for other hosts requiring BOOTP services.

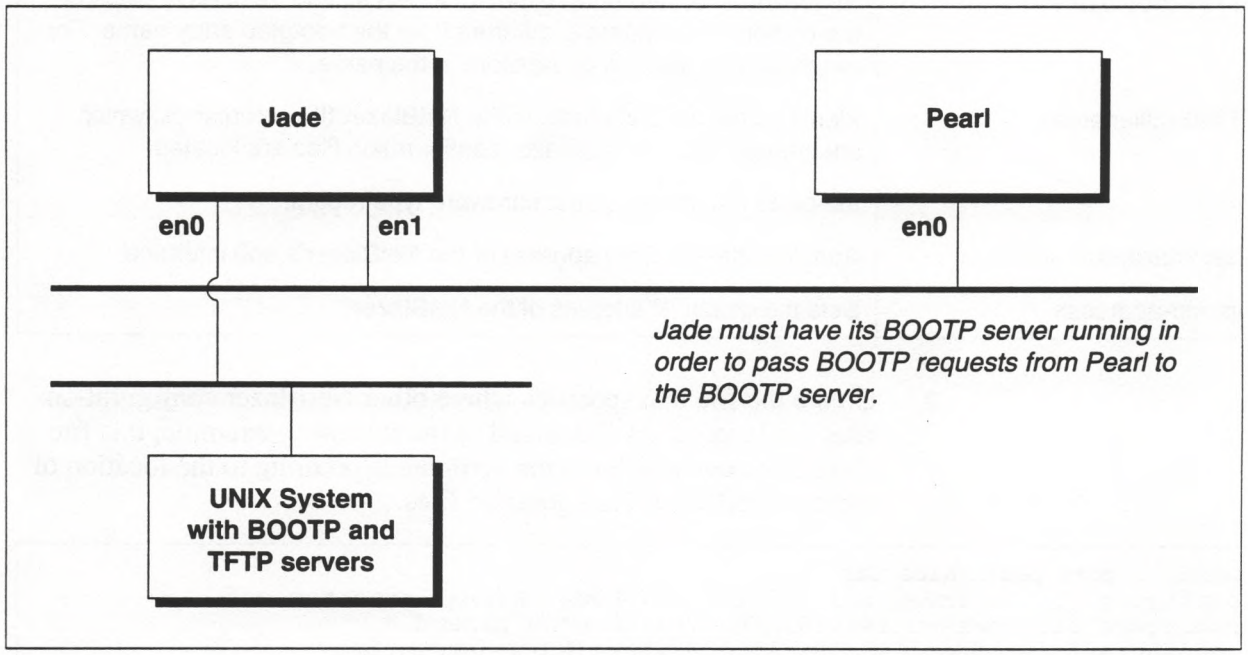


Figure 14-1. BOOTP Configuration Example

The following procedure describes how to set up BOOTP and TFTP services for the NetBlazer named pearl in Figure 14-1.

1. Add the following entry to the /etc/bootptab file on the UNIX system with the BOOTP and TFTP servers. Refer to Table 14-1 for a description of the parameters used in a NetBlazer's /etc/bootptab record.

```
pearl:\
        :hd=/home/NB:bf=fred:sm=255.255.255.0:\
        :hn:T140="pearl/site.cnf":\
        :ht=1:ha=0080ad021300:ip=143.191.63.1:
```

Table 14-1. Bootptab Field Definitions

Field	Description
<record-name>	The name of the bootptab entry should be the host name of the NetBlazer without any underscores.
hd=<home-directory>	Identifies the directory that contains the file fred and any other configuration files you are using remotely.
bf=<boot-file>	Identifies the NetBlazer boot file – fred.
sm=<subnet-mask>	Sets the subnet mask in dotted decimal notation (e.g. 255.255.255.0).
hn	Sends the host name specified by the bootptab entry to the NetBlazer.
T12=<hostname>	Sends the specified host name. This field should be used in place of the hn field if hostname is different from the bootptab entry name. For example, you want an underscore in the name.
T140=<filename>	Identifies the file that contains the NetBlazer **file** commands, which specify where other NetBlazer configuration files are located.
ht=1	Indicates that this is a host hardware type record.
ha=<hardware-address>	Specifies the ethernet address of the NetBlazer's en0 interface.
ip=<ip-address>	Sets the global IP address of the NetBlazer.

2. Create the file that specifies where other NetBlazer configuration files are located. As illustrated in the following example, this file should include **configure file** commands pointing to the location of various NetBlazer configuration files.

```
napa: > more pearl/site.cnf
configure file startup 143.191.10.100:/home/NB/pearl/startup.cnf
configure file passwd 143.191.10.100:/home/NB/passwd
configure file modem 143.191.10.100:/home/NB/modemcap.txt
configure file chat 143.191.10.100:/home/NB/chat.txt
configure file default 143.191.10.100:/home/NB/default.cnf
configure file token 143.191.10.100:/home/NB/token002.mcd
configure file overlay 143.191.10.100:/home/NB
```

3. Using FTP, copy the NetBlazer's software (fred) and configuration files into the appropriate directories on the UNIX host.

Note: *All files used to boot and configure a NetBlazer must be readable by everyone. If you use* ***save remote*** *to update the passwd and/or startup.cnf files, these files also must be writable by everyone.*

4. Make sure that you have the appropriate TFTP and BOOTP entries in the /etc/inetd.conf and /etc/services files on the host system. The following display shows typical entries for these two files.

```
napa: > grep -y boot /etc/inetd.conf
# Tftp service is provided primarily for booting.  Most sites run this
# only on machines acting as boot servers.
tftp    dgram   udp     wait    root    /usr/etc/in.tftpd       in.tftpd
/tftpboot
# BOOTPD
bootps  dgram   udp     wait    root    /usr/etc/bootpd         bootpd

napa: > grep -y boot /etc/services
# BOOTP
bootps          67/udp          bootp
bootpc          68/udp
```

5. Make sure TFTP is working by running **tftp** on the UNIX host.

```
napa: > tftp napa
tftp> get /home/NB/fred /dev/null
Received 664056 bytes in 14.9 seconds
tftp> quit
```

6. Enter a **boot bootp** command to configure the NetBlazer to load BOOTP instead of FRED as it normally does.

```
pearl:Top> boot bootp 60
boot bootp 60 (seconds)
```

This command tells the NetBlazer to attempt to boot from a BOOTP server on the network. If after 60 seconds it is unsuccessful, the NetBlazer will load FRED from the system diskette.

7. The final step in our example is to turn on the BOOTP server on jade to forward BOOTP requests from pearl to the UNIX host.

```
jade:Top> server start bootp 143.191.10.100
```

Using Remote Configuration Files

An alternative to using the BOOTP facilities is to put some or all of the NetBlazer configuration files on a UNIX system, and use TFTP to access these files. To do this you must put a FILES.CNF file on the NetBlazer system diskette. As illustrated in the following display, FILES.CNF should include a series of **file** commands that specify the location of the various configuration files.

```
pearl:Top> more files.cnf
configure file startup startup.cnf
configure file passwd 143.191.10.100:/home/NB/passwd
configure file modem 143.191.10.100:/home/NB/modemcap.txt
configure file chat 143.191.10.100:/home/NB/chat.txt
configure file default 143.191.10.100:/home/NB/default.cnf
configure file token 143.191.10.100:/home/NB/token002.mcd
configure file overlay 143.191.10.100:/home/NB
```

By executing the commands in FILES.CNF before the STARTUP.CNF commands, the NetBlazer learns where to look for the configuration files.

Note: *You must use the IP address of the remote host in FILES.CNF because the NetBlazer is not far enough in the configuration process to use the domain name service.*

Any NetBlazer command that operates on a NetBlazer file can be used with a remote file by specifying the <host>:<pathname> of the file. For example, entering **more napa:/home/NB/passwd** displays the contents of the passwd file in the home/NB directory on the host named napa.

To save changes to the current configuration settings and/or user records to a remote host, either issue a **save remote** command, or issue a **save local** command and use FTP to copy the file to the remote host. Although the first method is easier, it requires that the remote files be writable by everyone. If this presents a security problem, use the second method.

Using Local and Remote Password Files

In its simplest configuration, the NetBlazer loads the user records from the PASSWD file on the diskette at boot time. However, you can configure the NetBlazer to get user records from a PASSWD file on a remote IP host at boot time, or to look for a user ID in a remote PASSWD file if the user is not found in the local user list. Another option is to configure the NetBlazer to query a domain name server for user records that are not found in the local or remote PASSWD file.

Note: *Temporary user records, acquired from a remote PASSWD file or domain name server, are not saved by the* ***save*** *command and cannot be changed unless you first make the user record local using the* ***user local*** *command.*

Loading a Remote Password File at Boot Time

When the NetBlazer is booted from the system diskette, it gets the location of the various NetBlazer configuration files (including the PASSWD file) from the FILES.CNF file before running the STARTUP.CNF file.

To configure the NetBlazer to load a password file from a remote IP host at boot time, you must set up a FILES.CNF file that includes a **files passwd** command entry that points to the location of the remote PASSWD file.

During the boot process, the NetBlazer loads the user information from the remote PASSWD file, identified in the FILES.CNF file, into the user list area of the NetBlazer's internal memory.

Note: *If you modify or add to the user list, you must make sure that the remote PASSWD file is updated to reflect the most recent user list. You can do this either by issuing a* ***save remote*** *command, or by issuing a* ***save local*** *command and using FTP to copy the PASSWD file to the remote host.*

Although the first method is easier, it requires that the remote PASSWD file be writable by everyone. If this presents a security problem, use the second method discussed above.

Using a Remote Password File in Addition to the Local Passwd File

User records that are loaded into the NetBlazer's memory during the boot process are treated as local user records in that they can be modified and saved in the PASSWD file.

You can configure the NetBlazer to look for a user record in a remote PASSWD file if the user is not found in the local user list. Entering a **user remote** <host>:<filename> command tells the NetBlazer where to look for a user record that is not contained in the local user list.

```
NB:Top>Configure>User> remote napa:/home/NB/passwd
remote password file: napa:/home/NB/passwd
```

The above command allows the NetBlazer to check the /home/NB/passwd file on the remote system named napa if a valid user ID is not found in the local user list. If the user ID is found in the remote PASSWD file, the user is temporarily added to the list of users until the user logs out of the NetBlazer.

Refer to the **user remote** command description in the *NetBlazer Command Reference Manual* for additional information on setting up and using a remote PASSWD file.

Getting Password Records from a Domain Name Server

You can configure the NetBlazer to query a DNS if a user is not found in either the local or remote PASSWD files.

To set up a domain name server to send password records to the NetBlazer, you need to add IN-class TXT records to the server. Each record, accessed by user name, must contain a complete password line in the TXT record.

To enable DNS queries for user records, enter the following command:

```
NB:Top>Configure>User> domainlookup on
Domain lookup is enabled
```

To keep user records separate from host records, you should set up a separate domain for user records. This allows you to have users and hosts with the same name in the domain name server.

The **user userdomain** command tells the NetBlazer which domain suffix to use when looking for a remote passwd entry in DNS.

```
NB:Top>Configure>User> userdomain txt.telebit.com
user lookup domain: txt.telebit.com
```

If the user ID is not found in the local or remote PASSWD file, the NetBlazer queries the domain name suffix specified by the **userdomain** <domainname> command for the user record. If you do not specify a domain name suffix, the NetBlazer uses the same server used for other DNS queries.

Using Syslog to Monitor NetBlazer Activity

You can configure the NetBlazer to send syslog messages to a UNIX host, the NetBlazer console, your login terminal, and/or an internal buffer in the NetBlazer's memory. Messages stored in memory can be listed to a disk file or to your terminal screen.

This section explains how to configure the NetBlazer to send syslog messages to a UNIX host. For information on sending syslog messages to the other destinations, refer to the **syslog** command description in the *NetBlazer Command Reference Manual.*

Sending Syslog Messages to a UNIX Host

The **syslog host** command controls sending NetBlazer activity information to a UNIX system's *syslogd* daemon, which then forwards this information to the appropriate system log files and/or users.

```
NB:Top>Configure>Syslog> host on byron local0
sending syslog messages to byron(143.191.10.243), facility = local0
```

The above example shows you how to configure the NetBlazer to send syslog messages to a UNIX host named byron using the local0 facility.

As illustrated in Figure 14-2, the */etc/syslog.conf* file on the UNIX system controls where the NetBlazer messages are sent.

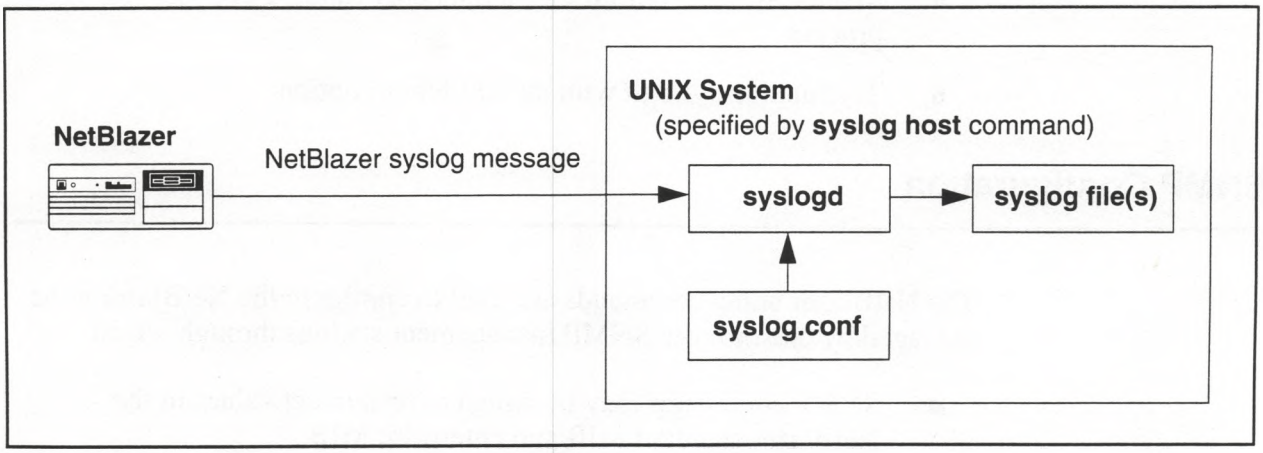


Figure 14-2. Sending Syslog Messages to a UNIX Host

For information on setting up your UNIX host system, see the following UNIX manual pages: *syslog*, *syslogd*, *syslog.conf*.

Verifying that Syslog Messages Are Reaching the Host

You can verify that syslog messages from the NetBlazer are reaching the right file on the host system by issuing a **msglog** <message> command. The <message> parameter may be a single word or several words enclosed in quotes as shown in the following example.

```
NB:Top>Configure>Syslog> msglog "message from NetBlazer"
```

If the message sent by the **msglog** command does not reach the host log file, try the following:

1. Enter a **syslog list** command to verify that the NetBlazer's syslog messages are being sent to the correct UNIX host.

2. Enter a **interface trace** <interface>**out** command where <interface> specifies the name of the interface that syslog messages will be sent through. Then, send your syslog message again to verify that the message is going out.

   If you do not see trace information about the message, verify that you have the interface and route set correctly to reach the host.

3. Verify that your */etc/syslog.conf* configuration file on the host is set up correctly to route messages from the NetBlazer to the appropriate log file. You should have a line in your */etc/syslog.conf* file similar to the following:

   local0.debug /var/log/netblazer

4. Make sure that the log file, /var/log/netblazer in the above example, is present on your host system.

5. Make sure that your host system is only running one *syslogd* process.

6. Try running *syslogd* with the *-d* (debug) option.

SNMP Configuration

The NetBlazer **snmp** commands are used to configure the NetBlazer to be managed by one or more SNMP management stations through which:

- SNMP commands may be issued to read or set values in the NetBlazer standard MIB and enterprise MIB.
- Authentication and modem traps can be switched on or off. Authentication traps are used to report receipt of an invalid community group name attempting to issue an SNMP command. Modem traps (call start, call stop and modem change) are sent to the trap community in the event they occur.
- Administrative information can be obtained, including system name, contact (name and phone number), and its physical location.

Default Settings

When initially powered on, the NetBlazer defaults are:

- Enterprise MIB enabled with read|write permission
- Community setting permits any host to access the Enterprise MIB

The NetBlazer distribution diskettes are furnished with SNMP default settings for two communities: public and private.

- Public – read only
- Private – read/write

Community Groups and Security

Before a management station can issue an SNMP command to a NetBlazer, the NetBlazer must be configured to recognize one or more management stations. This is accomplished by establishing an SNMP community name and a list that contains the host names of all management stations through which SNMP access to the NetBlazer is desired.

It is also possible to admit all hosts by not entering any hosts. Community names are thus somewhat like passwords. SNMP commands can directly access (get or set) objects and variables in the NetBlazer's MIB-II and enterprise MIB. Permissions of read only or read/write are assigned on a per community basis.

Community names can be up to 31 characters long. Note, however, that if spaces or special characters are used, it is necessary to surround them with double quotes in order for the NetBlazer to see the string as one argument.

The special trap community receives authentication, modem traps, and startup traps and is created by not specifying any [<ro>|<rw>] privilege. Note that only one trap community can exist. A newly added trap community name replaces the previous name. Refer to the SNMP Command section in the *NetBlazer Command Reference Manual* for further details.

The Telebit Enterprise MIB

Because the configurability in MIB-II is limited (with respect to the NetBlazer's functionality), an enterprise MIB was developed to provide extended configurability. This approach provides nearly complete configurability of the NetBlazer for both Telebit's NetBlazer Configuration Utility, and network management stations.

System Administrators wishing to directly access the Telebit enterprise MIB using their SNMP network management software are directed to the text file that makes up the Telebit enterprise MIB. This file is on the Utility distribution diskette, and is heavily commented to provide adequate information for persons knowledgable in integrating managed object MIBs into network management applications.

The **snmp enterprise** command is provided to either enable or disable SNMP access to the enterprise MIB.

Three levels of SNMP access privileges to the NetBlazer's enterprise MIB are provided: Read only, Read/Write, and Enterprise MIB switched off.

Notes:

1. *If you plan to use the Telebit NetBlazer Configuration Utility, the Enterprise MIB must permit read\write access.*

2. *If you plan to use the Telebit enterprise MIB with a network management station, refer to the documentation provided with your MIB compiler or contact your vendor for more information about how to use the Telebit MIB with a third party MIB compiler. You may also contact Telebit Technical Support department at 1-800-TELEBIT.*

SNMP Configuration Procedure

1. The default SNMP private community has read/write privileges enabled and therefore represents a security exposure. You can either delete the default private community (eliminating read/write access for all stations using the private community), or limit access to a specific list of hosts in order to eliminate the security exposure. To delete the private community, use the **snmp community delete** command.

```
opal:Top>Configure>SNMP>Community> delete private
```

2. Add the name of the new community desired along with the access (read only or read/write) using the **snmp community add** command.

Note: *If you do **not** specify rw or ro, the new community name will default to the trap community.*

```
opal:Top>Configure>SNMP>Community> add Denver rw
```

3. Add the IP and IPX host(s) that will reside within the new community name using the **snmp community host** command.

```
opal:Top>Configure>SNMP>Community> host Denver add ip 143.191.11.5
opal:Top>Configure>SNMP>Community> host Denver add ipx 331.1
```

4. Set the enterprise MIB to the desired state (disabled, or enabled with read only, or enabled with read|write access) with the **snmp enterprise** command.

```
opal:Top>Configure>SNMP> enterprise enable rw
```

The default condition of the enterprise MIB is enabled with read/write permission enabled, however, the default condition will not be recorded in a **save** operation.

When disabled, the enterprise MIB appears nonexistent. SNMP requests for variables contained in the MIB receive a return message that the variable does not exist.

5. Enter the System Contact using the **snmp sysContact** command.

```
opal:Top>Configure>SNMP> sysContact Geraldo Headcrash 555-4357
```

The **snmp sysContact** command sets the string that is transmitted to a remote management station when the sysContact variable is queried. This should be set to the name and phone number of the person responsible for the operation of the NetBlazer to which the query is directed. The default value for <sysContact-string> is an empty string.

6. Enter the System Location using the **snmp sysLocation** command.

```
opal:Top>Configure>SNMP> sysLocation TechPubs Lab, Bldg 1, 2nd Flr
```

The **snmp sysLocation** command sets the string that is transmitted to a remote management station when the sysLocation variable is queried. This should be set to the physical and logical location of the NetBlazer to which the query is directed. The default value for <sysLocation-string> is an empty string.

7. Enter the SNMP System Name using the **snmp sysName** command.

```
opal:Top>Configure>SNMP> sysName Opal, 143.191.64.17
```

The **snmp sysName** command sets the string that is transmitted to a remote management station when the sysName variable is queried. This should be set to the domain name and/or IP address of the NetBlazer to which the query is directed. The default value for <sysName-string> is an empty string.

By convention (in SNMP), sysName is the full domain name of the device. However you are may use whatever string that is appropriate to your use.

8. Verify your entries by performing an **snmp list.**

```
opal:Top>Configure>SNMP> list
( 1)snmpInPkts                      0     ( 2)snmpOutPkts                      0
( 3)snmpInBadVersions               0     ( 4)snmpInBadCommunityNames          0
( 5)snmpInBadCommunityUses          0     ( 6)snmpInASNParseErrs               0
( 7)                                0     ( 8)snmpInTooBigs                    0
( 9)snmpInNoSuchNames               0     (10)snmpInBadValues                  0
(11)snmpInReadOnlys                 0     (12)snmpInGenErrs                    0
(13)snmpInTotalReqVars              0     (14)snmpInTotalSetVars               0
(15)snmpInGetRequests               0     (16)snmpInGetNexts                   0
(17)snmpInSetRequests               0     (18)snmpInGetResponses               0
(19)snmpInTraps                     0     (20)snmpOutTooBigs                   0
(21)snmpOutNoSuchNames              0     (22)snmpOutBadValues                 0
(23)                                0     (24)snmpOutGenErrs                   0
(25)snmpOutGetRequests              0     (26)snmpOutGetNexts                  0
(27)snmpOutSetRequests              0     (28)snmpOutGetResponses              0
(29)snmpOutTraps                    0     (30)snmpEnableAuthenTraps    disabled
SNMP UDP server is enabled
SNMP IPX server is disabled
sysDescr: Telebit NetBlazer Version 1.92x2-beta
sysLocation: TechPubs Lab, Bldg 1, 2nd Flr
sysContact: Geraldo Headcrash 555-4357
sysName: Opal, 143.191.64.17
Telebit enterprise MIB is enabled read-write
Startup traps are disabled
Authentication traps are disabled
```

9. Save the new SNMP configuration information with the **save** command.

```
opal:Top>Configure> save
Saved startup file 'startup.cnf'.
Saved passwd file 'passwd'.
opal:Top>Configure>
```

NetBlazer™

IPX Configuration

IPX Configuration 15

This chapter provides instructions on how to configure the NetBlazer to route IPX packets between local networks and over a dynamic dial-up interface. To find these instructions useful, you need to be familiar with your IPX network and the terms that refer to it.

To route IPX packets between local networks, you need to assign an IPX address to the NetBlazer. You should verify the NetBlazer's host name and assign an internal network number to the NetBlazer. Also, you need to know the network addresses of each Ethernet and/or Token Ring LAN that is attached directly to the NetBlazer.

You need to decide how the NetBlazer will advertise and learn about servers. You also need to decide how the NetBlazer will broadcast and learn routes to other LANs that are not directly accessible to the NetBlazer. You have two choices: Manually add static routes to the NetBlazer's routing table or configure the NetBlazer to dynamically learn the routes to other indirect networks using RIP.

Tip: *Static routes work best for small, stable networks with just a few routes. For complex networks with many paths, like the network shown in Figure 15-1, RIP provides a more flexible and easier way to maintain the list of routes used by the NetBlazer.*

This chapter describes the following tasks:

- Verify the host name of the NetBlazer.
- Assign an internal network number and an IPX address to the NetBlazer.
- Add interfaces and assign an IPX address to each interface.
- Configure the NetBlazer to use IPX Service Advertising Protocol (SAP).
- Configure the NetBlazer to use IPX RIP.
- Configure a dynamic IPX interface.
- Save the NetBlazer System Configuration.
- Configure the remote NetBlazer.
- Use the Remote Shell.

Go on to configure a NetBlazer (topaz, shown in Figure 15-1) to route IPX packets between LANs.

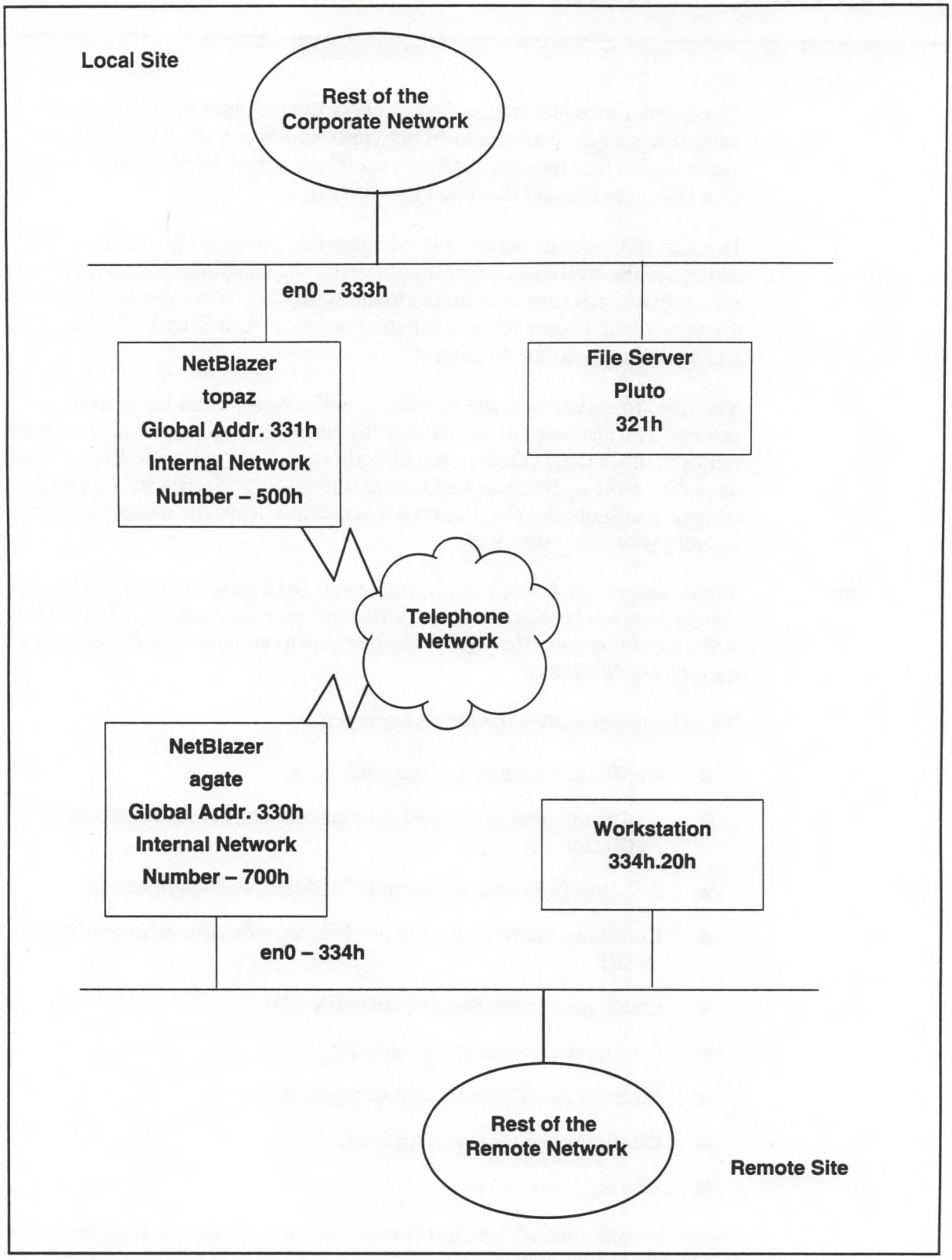


Figure 15-1. IPX Network Example

Verifying the Host Name

Host Name

Chapter 2, Getting Started, tells you how to assign a host name to the NetBlazer. Go to the Configure command level and verify the host name as shown below:

```
topaz:Top> configure
topaz:Top>Configure> hostname
```

The host name of the NetBlazer in the above example is topaz. It is displayed as part of the command prompt.

Assigning an Internal Network Number and IPX Address

IPX Numbering and Addressing

Before assigning IPX numbers and addresses to the NetBlazer, you can learn about such numbers and addresses in this section. Work with your network administrator in assigning these numbers and addresses. See the description of the **ipx address** command in the *NetBlazer Command Reference Manual*.

IPX Address

An IPX address is the unique identifier for an IPX network and a particular node on the network. (See Table IPX-1 under the **ipx address** command in the IPX Command section of the *NetBlazer Command Reference Manual*.)

IPX Network Number

An IPX network number is an address. A network number uniquely identifies a network. A network number is an 8-digit hexadecimal in the 1 to FFFFFFFE range (omit leading zeros). This manual shows a hexadecimal number this way: 500hex or simply 500h with the "hex" or the letter h indicating hexadecimal. However, do not enter hex or h when entering an IPX network number to the NetBlazer.

When you assign an IPX network number to an interface such as en0 (an Ethernet card), the NetBlazer finds the media-access control protocol (MAC) address of the device. For example, you can assign the network number 333hex to en0. The NetBlazer finds the MAC address of en0, that is, C0703420hex, and it is en0's IPX node number. The full IPX address of en0 is 333.C0703420 in hexadecimal.

When you assign an IPX network number or address to a NetBlazer, the NetBlazer assigns a random node number. For example, you can assign the network number 331hex to the NetBlazer. The NetBlazer assigns the node number of CEE2hex. Its full IPX address is 331.CEE2 in hexadecimal.

IPX Internal Network Number

An IPX internal network number uniquely identifies a logical network that may or may not be the same as a physical network. An internal network number is an 8-digit hexadecimal similar to an IPX network number.

IPX Node Number

An IPX node number uniquely identifies an individual station on a network. A node number is a 12-digit hexadecimal in the 1 to FFFFFFFFFFFE range (omit leading zeros), such as, CEE2h, CO703420h, or simply 1h. A station on a network can be a workstation, a file server, or a router such as a NetBlazer.

A node number follows a network number. Together, the network number and the node number make up the IPX address of a station, such as a NetBlazer, on a network.

IPX Port Number

An IPX address can have a third part – the port or socket number. A port number is a 4-digit hexadecimal in the 1 to FFFE range (omit leading zeros). Every IPX address does not have a port number, for example, an interface address has only two parts.

Stations such as file servers have port or socket numbers. For example, a file server can have the address 321.1.451 in hexadecimal.

Some IPX socket numbers such as the socket number for a server are standardized (see Table IPX-2 under the **ipx sap table add** command in the IPX Command section of the *NetBlazer Command Reference Manual*).

Assigning an Internal Network Number

Go to the IPX command level and assign an internal network number to the NetBlazer as shown below:

```
topaz:Top>Configure> ipx
topaz:Top>Configure>IPX> internal-net 500
IPX Internal Network is 500
```

The internal network number is 500hex in the above example. The internal network number must be unique. Only IPX WAN and the optional NetBlazer/ACS use the internal network number.

Assigning an IPX Address

At the Configure IPX command level, enter the IPX address assigned to the NetBlazer:

```
topaz:Top>Configure>IPX> address 331
Global IPX address is 331.CEE2
```

The NetBlazer's global IPX address is 331h.CEE2h. In this example, the NetBlazer assigned the host (or node) number of CEE2h.

Note: *The IPX address used in this example and other examples throughout this manual are for illustrative purposes only. Use your own IPX addresses when configuring the NetBlazer.*

Adding Interfaces and Assigning an IPX Address to Each Interface

First, add an interface for each Ethernet and/or Token Ring board installed in the system. Then, assign an IPX address.

Adding Interfaces

At the Configure IPX command level, add an interface for each Ethernet and/or Token Ring board installed in the system as shown below.

```
topaz:Top>Configure>IPX> add en0
IPX INITIALIZED
Added interface en0 for IPX
```

This command adds the en0 interface for use by IPX. Enter **add en1** if you have a second Ethernet board. The interface names for Token Ring boards are tr0 and tr1.

Assigning IPX Addresses to Interfaces

At the Configure IPX command level, assign an IPX address to each interface as shown below.

```
topaz:Top>Configure>IPX> address 333 en0
```

This command assigns IPX address 333h to the en0 interface. Make sure the IPX network number you give each Ethernet and Token Ring interface matches the network's IPX address for that interface.

To see the effects of the above **ipx address** command, enter the **list** command and then the **route list** command.

```
topaz:Top>Configure>IPX> list
Name          Mtu   Network     Address         Ipkts Ierrs    Opkts Oerrs Type
iptunnel*     604   331         CEE2                0     0        0     0   31
en0           1500  333         C0703420            2     0        2     0 Enet
topaz:Top>Configure>IPX> route list
Routing tables
Destination       Gateway             Flags   Refs     Use Hops Ticks Interface
333.*             333.C0703420        U          1       0    0     1  en0
```

Notice that the NetBlazer assigned the host (or node) number of C0703420h to the IPX address of the en0 interface; its address is 333h.C0703420h.

Specifying Packet Frames

To specify the link-layer frame type for an Ethernet or Token Ring interface, go to the Configure IPX Frames command level and enter the frames specification for the interface.

```
topaz:Top>Configure>Interface> ipx
topaz:Top>Configure>IPX> frames en0 ethernet_2
```

This IPX frames command specifies Ethernet type 2 (Ethernet type 0x8137) packet frames. The default for Ethernet is Ethernet 802.3. If you use Ethernet II packets, use the **frames** <interface> **ethernet_2** command to specify the correct frames.

The default for Token Ring is Token Ring SNAP. If you have Token Ring and you have not changed the file server to Token Ring SNAP, use the **frames** <interface> **token-ring** command to specify the correct frames.

To display current framing for interface en0, for example, enter **frames en0**.

Configuring the NetBlazer to Use IPX SAP

SAP allows servers such as file servers and print servers to advertise their services and addresses. When servers come up, they advertise their services with SAP. When they are brought down, they use SAP to announce that their services are not available. The NetBlazer sets up and maintains an IPX server information table that lists the services available on the internetwork.

Listening for IPX SAP Information

The NetBlazer listens by default for IPX SAP information from servers on all of the NetBlazer's IPX interfaces.

If you do not want the NetBlazer to accept SAP information from servers on the interface(s), enter an **IPX SAP listen all off** command.

```
topaz:Top>Configure>IPX>SAP> listen all off
Stopped SAP Listens on 'en0'
```

This **IPX SAP listen** command causes the NetBlazer to stop listening for SAP information through all interfaces.

If you want the NetBlazer to listen for IPX SAP information from servers on only one interface, go to the Configure IPX SAP command level and enter an **IPX SAP listen** command for the interface.

```
topaz:Top>Configure>IPX> sap
topaz:Top>Configure>IPX>SAP> listen en0 on
SAP Listener Started
Started SAP Listens on 'en0'
```

The **IPX SAP listen** command causes the NetBlazer to listen for SAP information through the interface.

If you want the NetBlazer to listen again for IPX SAP information from servers on all of the NetBlazer's IPX interfaces, enter an **IPX SAP listen all on** command for all IPX interfaces.

```
topaz:Top>Configure>IPX>SAP> listen all on
Started SAP Listens on 'en0'
```

Broadcasting IPX SAP Information

To broadcast IPX SAP information for servers on this network to other IPX routers on an interface, go to the Configure IPX SAP command level and turn on IPX SAP broadcasts for each interface.

```
topaz:Top>Configure>IPX>SAP> add en0
Started SAP broadcasts on 'en0'
```

The **IPX SAP add** command causes the NetBlazer to send SAP information through each interface at one-minute intervals. One minute is the recommended interval. (A SAP entry at the remote end times out in about four minutes if an update is not received.)

Enter **list** at the Configure IPX SAP command level to verify your entries:

```
topaz:Top>Configure>IPX>SAP> list
Interface                Listen       Broadcast    Interval (minutes)
iptunnel                    On           Off
en0                         On           On             1
```

Enter **table list** at the Configure IPX SAP command level to see entries added by SAP. The file server on the segment has been added:

```
topaz:Top>Configure>IPX>SAP> table list
Type Server Name                Hops F Interface  Address
 4    PLUTO                        2   en0        00000321 000000000001 0451
```

Configuring the NetBlazer to Use IPX RIP

To send IPX packets to networks that are not connected directly to one of the NetBlazer's interfaces, the NetBlazer needs to know which interface to use to reach a particular destination network. This information is kept in the NetBlazer's IPX routing table. This table includes two types of entries, dynamic routes added by RIP and static routes entered by an operator.

Listening for IPX RIP Information

The NetBlazer listens by default for IPX RIP information from other IPX routers on all of the NetBlazer's IPX interfaces. Leave IPX listen on.

Broadcasting IPX RIP Information

To broadcast IPX RIP information to other IPX routers on an interface, go to the Configure IPX RIP command level and turn on IPX RIP broadcasts for each interface.

```
topaz:Top>Configure>IPX>RIP> add en0
RIP Broadcasts Started
Started RIP broadcasts on 'en0'
```

The **IPX RIP add** command causes the NetBlazer to send RIP information through each interface in one-minute intervals. One minute is the recommended interval. (A RIP entry at the remote end times out in about four minutes if an update is not received.)

Enter **list** at the Configure IPX RIP command level to verify your entries:

```
topaz:Top>Configure>IPX>RIP> list
Interface                Listen       Broadcast    Interval (minutes)
iptunnel                   On           Off
en0                        On           On             1
```

Sending IPX Packets Through an IP Tunnel

If you want to put IPX datagrams in IP packets to "tunnel" them through an IP network, use the **ipx iptunnel** command.

Adding a Peer IP Address

Go to the Configure IPX IpTunnel command level and enter the **add** command with a peer IP address as follows:

```
topaz:Top>Configure>IPX> iptunnel
topaz:Top>Configure>IPX>IpTunnel> add 143.191.11.5
```

The peer IP address is the IP address of a remote host to which the NetBlazer sends IPX packets.

Adding a Route for the IP Tunnel

To set up a route for the IP tunnel, enter the **iptunnel route** command with the IPX address of a server, such as a file server, on the destination IPX network and the peer IP address as follows:

```
topaz:Top>Configure>IPX>IpTunnel> route 321 143.191.11.5
```

For more information on the **ipx iptunnel** command, see the *NetBlazer Command Reference Manual.*

Be sure to set up IP routes between the local NetBlazer and the destination NetBlazer on an IPX network as shown in Figure 15-2. For information on IP addresses and routes, see the chapters on IP configuration in this guide.

When you have set up IP tunneling, the NetBlazer on the IPX network identifies which IPX packets to encapsulate in IP packets by checking the IPX routing table. When the IPX routing table shows a destination with the peer IP address you entered as an IP tunnel, the NetBlazer encapsulates the IPX packet in an IP packet and sends the IP packet to the NetBlazer on the IP network. That NetBlazer sends it on to the NetBlazer on the destination IPX network.

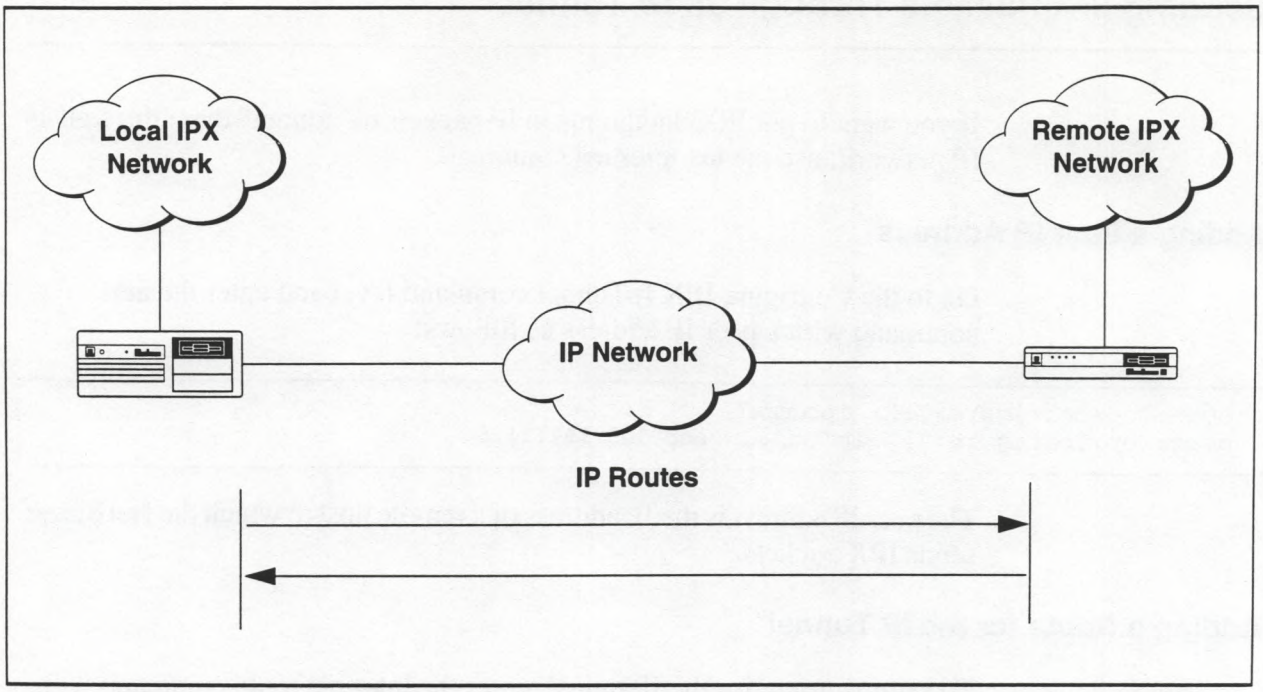


Figure 15-2. Routes for an IpTunnel

Configuring a Dynamic IPX Interface

When you set up a dynamic interface link, NetBlazers can encapsulate IPX packets in PPP frames and transfer them between local and remote sites over the telephone network. Both sites must use PPP framing.

For general information on configuring a dynamic interface, see Chapter 2, NetBlazer Interface Descriptions.

Setting Up a Dynamic Interface

You can set up a dynamic PPP interface between two NetBlazer routers, or between a remote workstation and the local NetBlazer (see Figure 15-3).

Notes: *If you already have a dynamic PPP interface on another protocol for the route you want to add, use that interface. You do not need to set up another interface to the same site for IPX. Just add the same interface to IPX and add an IPX route for the interface.*

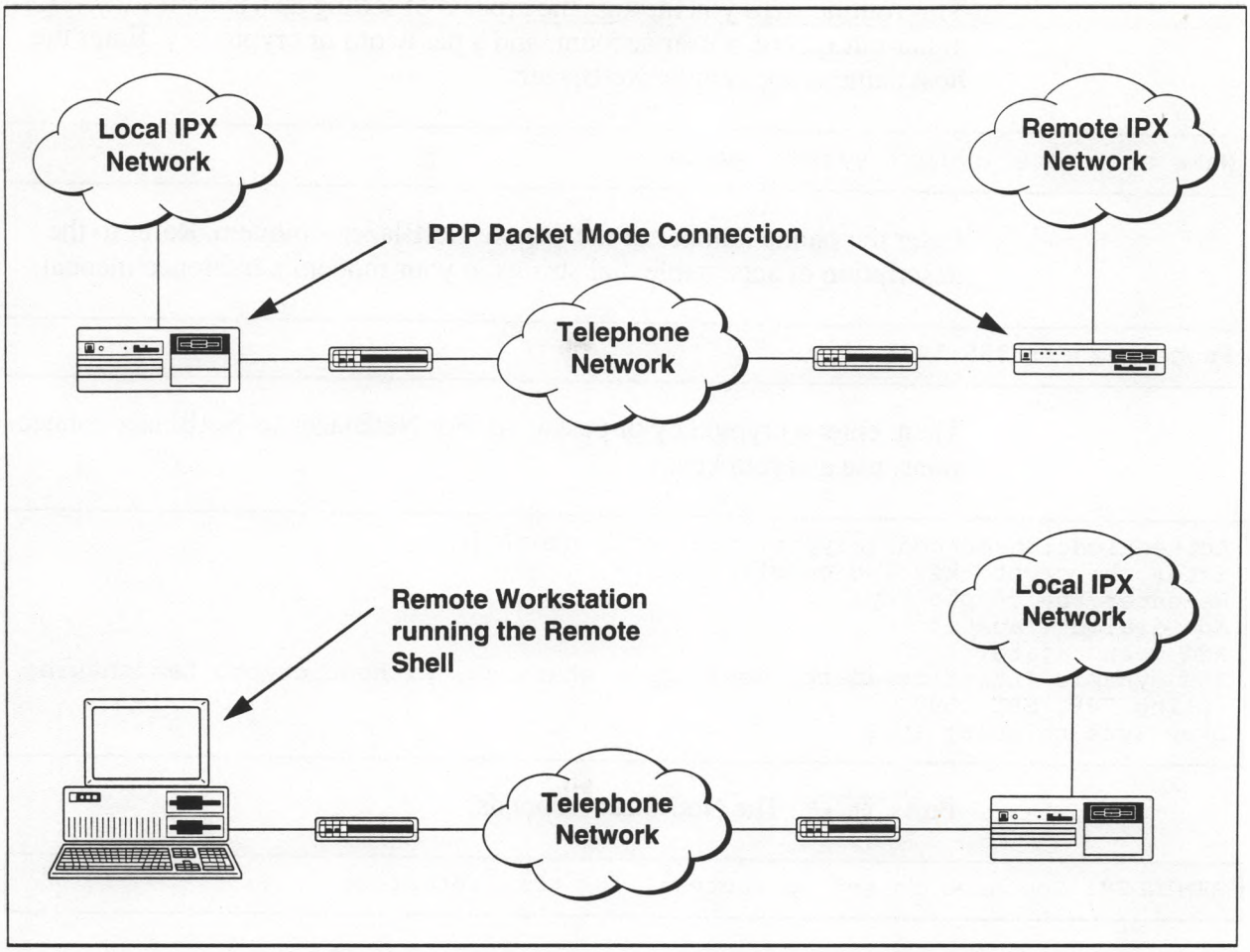


Figure 15-3. Dynamic IPX Interfaces

Use the **pppdial** command to set up a PPP connection between the local and remote sites. The **pppdial** command prompts you for information.

Notes: *If you are setting up a dynamic interface between a NetBlazer and a remote workstation, the workstation must use the Remote Shell. See the section titled Using the Remote Shell on page 15-17 in this chapter.*

Using Pppdial to Set Up a Dynamic Interface

The following example shows you how to use **pppdial** to set up a PPP dynamic interface between the two NetBlazers named agate and topaz shown in Figure 15-1.

Start by setting up on the local NetBlazer a dynamic interface named agate. Go to the Configure Interface Dynamic command level and enter **pppdial** at topaz's command prompt.

```
topaz:Top>Configure>Interface> dynamic
topaz:Top>Configure>Interface>Dynamic> pppdial
```

This routine steps you through the process of setting up a dynamic interface, a dial-out record, a user account, and a password or crypto key. Enter the host name of the remote NetBlazer.

```
Name of remote (other) system: agate
```

Enter the phone number of the remote NetBlazer's modem. Refer to the description of acceptable dial strings in your modem's reference manual.

```
Phone number: 555-3273
```

Then, enter a crypto key or password. For NetBlazer-to-NetBlazer connections, use a crypto key.

```
Authentication method (crypto, password, none) [c]:
Enter the crypto key (no echo):
Re-enter the crypto key:
Add dialout 'agate'
Add user 'agate'
Add dynamic interface=agate, user=topaz chat=ics, without crypto handshaking
 using PPP, MRU=1500
Okay (yes|no|quit) [y]?
```

Press ENTER. The NetBlazer responds:

```
REMINDER! You need to set up route(s) for this interface
```

Set idle time to six minutes or more as shown below:

```
topaz:Top>Configure>Interface>Dynamic> timeout agate 360
```

Adding a Route for the Dynamic Interface

Go to the Configure IPX command level. Use the **ipx add** command to add interfaces for the routes you intend to set up. This command has the following syntax:

ipx add <interface> [all]

The following example shows the addition of an interface:

```
topaz:Top>Configure>Interface>Dynamic> ipx
topaz:Top>Configure>IPX> add agate
Added interface agate for IPX
```

Use the **ipx route add** or **ipx route addprivate** commands to set up the routes. Use **ipx route addprivate** if you are using RIP and do not want a particular route advertised by RIP. Otherwise, use the **ipx route add** command. These two commands use the following syntax:

ipx route add <dest_addr> <interface> [<gateway> [<metric>]]

ipx route addprivate <dest_addr> <interface> [<gateway> [<metric>]]

Both commands require a destination IPX address and an interface name. A gateway IPX address and metric are also required if the destination network is more than one hop count away from the NetBlazer.

The following example shows you how to enter a route to agate:

```
topaz:Top>Configure>IPX> route
topaz:Top>Configure>IPX>Route> add 330 agate "" 1
```

Use the **ipx route listlocal** command to verify that you entered the route correctly.

```
topaz:Top>Configure>IPX>Route> listlocal
Routing tables
Destination     Gateway            Flags   Refs     Use   Hops Ticks
Interface
330.*           331.CEE2           UG        0        0     1   36  agate
333.*           333.C0703420       U         1        0     0    1  en0
```

The new entry shows the route to interface agate. Network 330h (agate's global IPX address; see Figure 15-1) is one hop away from the NetBlazer topaz. IPX packets destined for this network are sent through gateway 331h.CEE2h.

Viewing the Results

To see the results of running the **pppdial** routine and adding the route to agate, enter the four commands shown in the following example to produce lists of the interface, routes, dial-out, and users.

```
topaz:Top> interface list agate
Name                IP address    MRU   MTU type      line     pkts in  pkts out
agate                  0.0.0.0   1500  1500 DYN_PPP   Down           0         0
Idle: In 0:01:14:19    Out 0:01:14:19                     IP:
0          0
Will save 'agate' vj: auto
Current vj: not active
Interface = Dynamic PPP     Uname = topaz         Password = xyz
Dial-out = Yes         Dial-in = Yes
Chat script = ics      Crypto key = <<NONE>>      MRU = 1500      MTU=1500
Timeout = 360 s        Queue-max = 8
Cost = 1000          Bytespertick = 0
topaz:Top> ipx route list |grep agate
334.*              331.CEE2            UG        0         0    1   36  agate
topaz:Top> dialout list |grep agate
agate              555-3273          dialout
topaz:Top> user list |grep agate
agate                                          dial PPP    DRT
```

Note that the dial-out record shown above can be used to establish a character-mode connection as well as a packet-mode connection.

Saving the NetBlazer System Configuration

Make sure that your working copy of the NetBlazer system diskette is inserted in the NetBlazer. Enter **configure save** at the command prompt to save the NetBlazer configuration to diskette.

```
topaz:Top> configure save
Saved startup file 'startup.cnf'.
Saved passwd file 'passwd'.
```

Any time you modify the NetBlazer configuration, use the **configure save** command to update the STARTUP.CNF file on your NetBlazer system diskette.

Configuring the Remote NetBlazer

After setting up a PPP dynamic interface on the local NetBlazer and saving its configuration, you must configure the remote NetBlazer. If the remote NetBlazer is installed and ready to accept calls, call the remote NetBlazer (agate in the example), configure it, run **pppdial**, and save the remote NetBlazer's configuration. Use the same crypto key or password that you used for the local NetBlazer. Configuring the remote NetBlazer is similar to configuring your local NetBlazer; you can follow the steps in this chapter when you configure the remote router.

The interfaces between the two NetBlazers (topaz and agate in the example) are now ready to be used for packet-mode connections.

IPX Pinging Between NetBlazers

If you send IPX echo requests between the NetBlazers with the **ipx ping** command, you may have to enter the command a second time for it to start. On agate in the example, enter **ipx ping 331.CEE2**. The global IPX address of topaz is 331h.CEE2h.

Enter **^C** (control-C) to stop the ping session. If the first attempt to ping is not successful, enter **^C** and ping the NetBlazer a second time.

Adding a SAP Table Entry

If you want a workstation on a network (agate's network in the example; see Figure 15-1) to be able to communicate with a file server (Pluto in the example) on the other network (topaz's in the example), add a SAP table entry for the file server. Go to the Configure IPX SAP Table command level and enter the **add** command as follows:

```
agate:Top>Configure>IPX> sap table
agate:Top>Configure>IPX>SAP>Table> add
Server Name ? Pluto
Server Type ? 4
IPX Address ? 321.1.451
```

Your network administrator has probably given the file server a name; it is Pluto in this example. The server type you can see in Table IPX-5 under the **ipx sap table add** command in the *NetBlazer Command Reference Manual.* Ask your network administrator to get the server's IPX address by using the **ipx sap table list** command on the NetBlazer on the other network (topaz is the NetBlazer in the example). See page 15-8 for an **ipx sap table list** display.

Next, add a route to the file server as shown in this example:

```
agate:Top>Configure>IPX> route
agate:Top>Configure>IPX>Route> add 321 topaz "" 2
```

Keeping a Connection Open

A NetWare file server sends keep-alive packets that check whether a workstation is "alive," that is, working. This keeps the logical connection open. Often, the workstation is logged into the server over a dial-up link but is not communicating with the server.

With **ipx keepalive** started, the NetBlazer at the workstation end keeps the logical connection open when the physical dial-up connection is closed. The NetBlazer is shipped with **ipx keepalive** started.

Use the **ipx keepalive timeout** command to set the maximum time for sending IPX keep-alive packets.

```
agate:Top>Configure>IPX>Keepalive> timeout 120
agate:Top>Configure>IPX>Keepalive> timeout
Maximum Keepalive Time: 120 minutes
```

You can enter only **timeout** to see the current period.

For more information on the **ipx keepalive** command, see the *NetBlazer Command Reference Manual.*

Introduction

The Remote Shell lets you communicate with a local LAN using a remote PC that is connected to a NetBlazer on the local LAN. This section shows you how to configure the NetBlazer on the local LAN as well as how to install and configure the Remote Shell. It also shows you how to call the NetBlazer and communicate with the network's file server.

Before You Start

Configure the NetBlazer that will receive the calls from the Remote Shell for IPX.

The Remote Shell software is on the NetBlazer utilities diskette. Make a working copy of the utilities diskette. Install the Remote Shell from the working copy of the utilities diskette to a remote PC.

The utilities diskette has seven files for the Remote Shell, COMPPP.EXE, IPXPPP.LAN, IPX.COM, PPPCFG.EXE, PPPCFG.HLP, PPPCFG.MDM, and WATCHPPP.EXE. The network administrator can add files to the diskette before giving it to the user at the remote site. Files you may want to add include (be sure to observe software licensing requirements): LOGIN.EXE, LOGOUT.EXE, and NETX.COM (or BNETX.COM) as well as CAPTURE.EXE, FILER.EXE, MAP.EXE, SYSCON.EXE, USERLIST.EXE, and WHOAMI.EXE. The remote user can use these files at the remote PC instead of waiting for the files to be downloaded from the IPX network's file server.

Setting Up a Remote Shell User

The following example shows you how to set up a PPP Remote Shell user on a NetBlazer. For this example, the Remote Shell is named Jupiter. Jupiter will call into the NetBlazer called topaz (see Figure 15-1).

Note: *The interface names, addresses, and subdirectory names used in this example and other examples throughout this manual are for illustrative purposes only. Use your own interface names, addresses, and subdirectory names when configuring the NetBlazer and the Remote Shell.*

Go to the Configure Interface Dynamic command level on the NetBlazer topaz. Set up a dynamic interface named Jupiter by entering the **add** command. Select PPP and accept the default of 1,500 for MRU.

```
topaz:Top>Configure>Interface>Dynamic> add
Interface name: Jupiter
SLIP, PPP, or ARA (s|p|a) [s]: p
What is the Maximum Receive Unit (MRU) [1500]:
Add dynamic interface=Jupiter, using PPP, MRU=1500
Okay (yes|no|quit) [y]? y
```

Then, set up a user by entering the **user add** command at the Top level. Enter a password or a crypto key if you wish.

```
topaz:Top> user add
Enter the uname (1-32 chars): Jupiter
Want to enter a password [y]? n
Issue a crypto handshake [n]? n
User: Jupiter                privs:          dest-group:
Okay (yes|no|quit) [y]? y
```

Set idle time to six minutes (360 seconds) or more as shown below:

```
topaz:Top> dynamic timeout Jupiter 360
```

Adding an IPX Interface and Assigning an IPX Address to the Interface

Jupiter is now one of topaz's interfaces. Add an IPX interface to the NetBlazer topaz with the **ipx add** command. Then, assign Jupiter the same address as topaz with the **ipx address** command.

```
topaz:Top> ipx add Jupiter
Added interface Jupiter for IPX
topaz:Top> ipx address 331 Jupiter
```

These commands add the interface Jupiter to IPX and assign IPX address 331hex to the interface Jupiter.

Installing the Remote Shell

You are ready to install the Remote Shell on a PC. The files to be installed are on the working copy of the NetBlazer utilities diskette. Add a subdirectory named, for example, PPPSHELL, for the Remote Shell files. Put this subdirectory in a path statement in the PC's AUTOEXEC.BAT file.

Insert the diskette in the A or B drive of the PC. Copy the files to your C drive. For example, if you use the A drive, type the following at the **C:** prompt:

copy a:*.* c:\pppshell ENTER

This DOS command copies the Remote Shell files into the subdirectory named PPPSHELL.

Configuring the Remote Shell

If you put the subdirectory in which you put the Remote Shell files (PPPSHELL in the example) in a path statement in the PC's AUTOEXEC.BAT file, begin with step 1 below to configure the Remote Shell. Otherwise, go to the subdirectory itself. Enter **dir** at the **C:** prompt if you wish to see a list of the files in the subdirectory. Follow these steps:

1. Type the following at the **C:** prompt:

   pppcfg [ENTER]

   If you want to use text instead of graphics mode, type the following at the **C:** prompt:

   pppcfg -t [ENTER]

   The Remote Shell Utility screen is displayed.

2. Move the cursor to **New** in the **File** menu. Press [ENTER]. This action opens your Remote Shell configuration file. The cursor moves to **Configuration**.

3. Move the cursor to **Modem and port setup**. Press [ENTER].

   The Modem and Port Setup window is displayed.

4. In this window you can set the port number, modem type, baud rate, and flow control. However, you may need to set only the modem type.

   Move the cursor to the option you want to change and press [SPACE] to see the choices. Move the cursor to your choice and press [ENTER].

   After making your choices, press [ESC]. The window disappears. The cursor returns to **Modem and port setup** in the **Configuration** menu.

5. Move the cursor to **System setup**. Press [ENTER].

   The System Setup window is displayed.

6. In this window, enter the phone number of the NetBlazer and its name. Also, enter the user name. You can enter a password and a crypto key, too. Make sure the user name, password, and crypto key match what was set up on the NetBlazer.

   For the example, type a NetBlazer name of **topaz**, its phone number **555-3272**, and a user name of **Jupiter**. Press [ESC]. The window disappears. The cursor returns to **System setup** in the **Configuration** menu.

7. Move the cursor to the **File** menu. Move the cursor to **Save as**. Press [ENTER].

   The Configuration File Name window is displayed.

8. Type a file name following DOS conventions. Do not type an extension. Press [ENTER]. The window disappears. The utility saves the file with the extension PPP. It looks like this in the subdirectory: YOURFILE.PPP.

9. Move the cursor in the **File** menu to **Exit**. Press [ENTER] twice. The DOS prompt is displayed.

You now have a Remote Shell configuration file. Remember its name because it is used in the first step of calling the NetBlazer.

Calling a NetBlazer with the Remote Shell

Calling a NetBlazer with the Remote Shell is a three-step process. You can put the DOS commands in these steps into a batch file.

1. At the **C:** prompt, type **comppp** and the name of a Remote Shell configuration file such as YOURFILE.PPP and press ENTER as follows.

```
C:PPPSHELL>comppp yourfile.ppp
Telebit PPP Communication Driver V2.0
Installation successful.
```

The Remote Shell responds as the display above shows.

2. Type **ipx** and press ENTER as follows.

```
C:PPPSHELL>ipx

Novell IPX/SPX v.3.10 (911121)
(C) Copyright 1985, 1991 Novell Inc. All Rights Reserved.

LAN Option: Telebit PPP Driver. V1.0 (920514)
Hardware Configuration: Auto Configuration.
```

The Remote Shell dials the NetBlazer and it responds in a manner similar to the display above.

3. To do this step, you must have the NETX.COM (NET3.COM, NET4.COM, NET5.COM, or BNETX.COM) file on your PC (see the Before You Start subsection earlier in this Using the Remote Shell section).

   Type **netx** and press ENTER as follows:

```
C:PPPSHELL>netx

NetWare V3.26 - Workstation Shell (920211)
(C) Copyright 1991 Novell Inc. All Rights Reserved.

Running on DOS V3.20
SHOW DOTS ON

Attached to server PLUTO
12-24-92 4:25:08 PM
```

The Remote Shell dials the NetBlazer and it responds in a manner similar to the display above.

Using the WATCHPPP.EXE Program

To avoid executing a program on the file server and waiting for the files to be downloaded from the file server to the remote PC, use the WATCHPPP program.

At the **C:** prompt, type **watchppp** and press ENTER.

WATCHPPP.EXE is now in the PC's memory. If you or an application requests an .EXE or .COM file on the file server, WATCHPPP displays the message **Warning: Program on file server. File size nnnnnKB (A)bort/(C)ontinue?**

Enter **a** to stop the request. Enter **c** to continue accessing the file.

Load WATCHPPP.EXE only after you have loaded IPX.COM.

Communicating with a File Server

To make this step faster, make sure the LOGIN.EXE file is on your PC's hard drive (see the Before You Start subsection earlier in this Using the Remote Shell section).

At the **C:** prompt you can communicate with the file server. Instead of logging in at the **F:** prompt of the file server (this can take about three minutes), at the **C:** prompt enter **login** and your user id. By using LOGIN.EXE on the C: drive to log in, you avoid reading the LOGIN.EXE file from the file server to your PC.

Logging Off and Closing the Session

To make this step faster, make sure the LOGOUT.EXE file is on your PC's hard drive (see the Before You Start subsection earlier in this Using the Remote Shell section).

To log off, type **logout** at the **C:** prompt and press ENTER.

Type **netx u** at the **C:** prompt to unload NETX.COM from memory. Press ENTER.

To disconnect the PPP link, type **pppcfg**. Move the cursor to **Link** on the Remote Shell Utility screen. Then, move the cursor to **Disconnect PPP link** and press ENTER.

COMPPP.EXE and IPX.COM are still in the PC's memory. To dial the NetBlazer again, enter **netx**. This means that, if the modem connection is lost, you can redial by entering **netx**.

If IPX.COM is in the PC's memory and you want to use a different configuration file with COMPPP.EXE, reboot your PC to remove both IPX.COM and COMPPP.EXE from memory.

Using the Remote Shell Management Utilities

To use the Remote Shell management utilities, follow these steps:

1. Type the following at the **C:** prompt (if the subdirectory in which you put the Remote Shell files is in a path statement in the PC's AUTOEXEC.BAT file; otherwise, go to the subdirectory first):

   pppcfg [ENTER]

   If you want to use text instead of graphics mode, type the following at the **C:** prompt:

   pppcfg -t [ENTER]

   The Remote Shell Utility screen is displayed.

2. Move the cursor to the **Management** menu. Press [ENTER]. To select an option, move the cursor to the name of one of the utilities and press [ENTER].

Using the Remote Shell Help

To use the Remote Shell help, follow these steps:

1. Type the following at the **C:** prompt (if the subdirectory in which you put the Remote Shell files is in a path statement in the PC's AUTOEXEC.BAT file; otherwise, go to the subdirectory first):

   pppcfg [ENTER]

   If you want to use text instead of graphics mode, type the following at the **C:** prompt:

   pppcfg -t [ENTER]

   The Remote Shell Utility screen is displayed.

2. Move the cursor to the **Help** menu. Press [ENTER]. Move the cursor to **Index**, **How to use help**, or **About PPPCFG**. Press [ENTER]. Explore.

To see help when you are using the configuration utility, press [F1] at any time. Press [ESC] to leave help.

NetBlazer™

AppleTalk Configuration

AppleTalk Configuration 16

This chapter provides instructions for configuring the NetBlazer's AppleTalk® protocol functions and features. This chapter is based on the assumptions that:

- Your hardware connections to modems, an administrator's workstation, or Ethernet port(s) have already been made and are up and running. If not, refer to your *NetBlazer Installation Guide* for instructions in performing these procedures.
- You have completed Chapter 3, Getting Started, and have logged onto the NetBlazer at the root level from a local or remote administrator's workstation.

Functionally, there are four basic configurations of the NetBlazer AppleTalk protocol. These include the NetBlazer as:

- A local router
- A wide area router
- An AppleTalk Remote Access (ARA) server
- A combination of the above

Setup of each of these basic configurations are described in this section.

Default Settings

As shipped from the factory, the following default conditions are on the NetBlazer distribution diskette:

- Ethernet port en0 is enabled with the AppleTalk protocol active as a nonrouter.
- The AppleTalk Data Stream Protocol (ADSP) server is on.

These defaults enable you to connect your NetBlazer's en0 port to an existing AppleTalk EtherTalk network where the NetBlazer will appear as a node. To configure the NetBlazer over the network, you need to use a Macintosh computer running a communications program such as MacTerminal 3.0 or PacerTerm that supports the Apple Communications Toolbox.

Alternately, a Macintosh computer running a communications package may be connected to one of the NetBlazer's serial ports either directly (using a Macintosh compatible null modem cable or through modems). This connection to a serial line, in effect, enables the Macintosh computer to become the console through which ARA users can be configured, or further configuration of the NetBlazer can be performed.

General

Preplanning

Before beginning the NetBlazer AppleTalk configuration procedure, you may want to prepare a plan detailing how you want the NetBlazer to work with your network.

Ground Up

If you are designing a new network from the ground up, you need to determine your network number or range and zone names. Generally, unless you have more than about 50 AppleTalk nodes on an Ethernet line, pick one network number (1–65,279 are legal numbers) as opposed to a range. Note that Apple has reserved the range from 65,280 to 65,534 for start-ups.

If you have a very large network, pick a range of one number for about every 50 nodes. For example, if you have 250 nodes, pick five network numbers (i.e., 1,000 to 1,004). Making the range too large can cause performance degradation in certain circumstances (routing information overhead increases); making it too small can slow down nodes that are starting up that are trying to attach to the network.

Zone names are typically selected on the basis of physical location or function. A small site may have a single zone name (i.e., Chicago Office), while a larger site may have several logical zones (i.e., Accounting, Engineering, Marketing, Customer Support, etc.).

For more information on AppleTalk network design, refer to the Apple publication *"Inside AppleTalk"*, second edition, published by Addison Wesley, 1990.

Add-On

If you are adding a NetBlazer with the AppleTalk protocol to an existing network through the Ethernet port, you can either obtain the network number to which the NetBlazer will be connected, or the NetBlazer can be configured as a nonseed router to automatically learn the network number.

If you plan to use the NetBlazer as an ARA server, you can also disable the routing function. This is the simplest AppleTalk configuration possible; no knowledge of network numbers and zones is necessary in this case.

Nonseed routers automatically learn about the AppleTalk networks and zones to which they are directly connected from seed routers. This information is dynamic as a function of Apple's Routing Table Maintenance Protocol (RTMP). Acquired RTMP information is maintained in the non-seed router's RTMP table where it is "aged" if not updated regularly. Routes not updated eventually age to "bad."

Seed routers maintain a static list of networks and zones to which they are connected. Network numbers and zones therefore must be known in order to establish the seed router.

Generally, configuring the NetBlazer as a nonseed router is not recommended unless there is some redundancy of seed routers. For example, if a network has a single seed router attached and a failure of this router occurs, eventually the nonseed routers will age and discard their routing information, thus bringing the whole network down.

The NetBlazer as an ARA Server

If your primary application is to use the NetBlazer as an ARA server, you need to know:

- The number of remote users that will be accessing the NetBlazer
- Their login names
- Their passwords
- Their zone access privileges and home zone
- Their callback telephone numbers (if callback is desired)
- The maximum connect time per user (if other than unlimited)
- The AppleTalk network number and zones to which each NetBlazer Ethernet port will be connected

Once ARA users have been established and the AppleTalk interface has been activated, a user is automatically connected to his or her home zone upon calling into the NetBlazer (the NetBlazer is transparent to the ARA user). Callback is also supported on a per user basis. ARA user activity may be logged through the NetBlazer's syslog command.

ARA users must have the Apple ARA software installed on their computers.

Modems

The number of modems you will need is directly related to the number of remote users the NetBlazer must support. This number is normally determined by the maximum number of remote users you expect to be calling in at the same time and the number of other network services provided by the NetBlazer.

Notes:

1. *Be sure the modems used on the incoming telephone lines work with ARA. ARA-compatible Telebit modems include the WorldBlazer, T3000, and T1600 modems running version LA7.03 (or later) firmware.*

2. *The use of NetBlazer ports 00, 01 and 02 for ARA is not recommended. Up to 24 ARA lines are available with the Telebit ASYN8 and ASYN8+, or multiple NM8 options.*

User Names

Because ARA users are maintained in the same database as all other NetBlazer users but are a separate class (in addition to character mode users, PPP, and SLIP users), it is necessary to use a unique user ID for each service. For example, if user Joe wants an IP character mode login and an ARA login, he will need two different user names.

Passwords

ARA passwords are stored in the NetBlazer's crypto key field and can be up to 8 characters in length. They can include spaces or any other special characters consistent with Apple naming conventions, but not colons.

The NetBlazer as a Dial-Up Router

If the NetBlazer will be used primarily as a dial-up router, you need to obtain:

- The AppleTalk network number and zones to which each NetBlazer Ethernet port will be connected (seed router only)
- The name and telephone number of the remote site

Learn Farside Routes?

AppleTalk routes are normally always dynamic as a function of RTMP. However, in order to perform on-demand dial-up connection to a remote site through packet mode (PPP) use, it is necessary to create static routes. Telebit provides two means of accomplishing this: the **route add** command and the **route learn** command.

Telebit provides the **route learn** and **route forget** commands as a convenience when dialing into large AppleTalk networks, where it is not practical to manually add and then delete a large number of routes. The **route learn** command automatically learns the farside routes over a PPP connection. This information is automatically acquired, added to the routing table, and tagged as learned routes. These routes can later be removed with the **route forget** command, if necessary.

Although static routes can be manually added with the **route add** command, there is little benefit to doing so over using the **route learn** command.

IP Encapsulation in DDP

The NetBlazer currently does not support IP encapsulation in DDP (known as MacIP or KIP). This technique is used to run TCP/IP over LocalTalk or ARA. In this circumstance, the IP packets are encapsulated in DDP and sent over LocalTalk or the remote access link. You must then have a DDP/IP gateway device on the network to strip off the DDP packet headers and convert them into IP packets.

System Administration Considerations

You should be aware that when adding ARA users through the **configure user add** command, two or three records are automatically created:

- Password record
- Dial-out record (only for callback)
- Dynamic interface record, including time limit record and home zone record

ARA users are normally deleted through the **configure user delete** command. Should you wish to delete an ARA user record, you can also delete the users interface name under the Configuration>dynamic> interface menu.

Configuring the NetBlazer's Ethernet Port

Whether you plan to use the NetBlazer as an ARA server, a dial-up router, or both, you must first connect the NetBlazer to your AppleTalk LAN through the Ethernet port. The *NetBlazer ST or 40 Installation Guide* provides step by step instructions for making this electrical connection.

Note: *For each AppleTalk Ethernet interface you establish (the maximum number of Ethernet adapter boards supported by the NetBlazer is three), you need to specify whether the NetBlazer will be a seed or nonseed router. If you do not specify nonseed router, you will also need the network number or range and the list of zones.*

If you wish to have the NetBlazer appear only as a node on the network and not perform routing, use the nonroute option. You may find this desirable when you use the NetBlazer only as an ARA server. Note that the nonroute option can only be used when a single Ethernet port is used.

If you use two or three Ethernet ports, you must use either seed or nonseed routing.

After you have made the Ethernet electrical connection to the NetBlazer, you must configure the NetBlazer to recognize the Ethernet port as an AppleTalk interface. To do so, perform the following procedure:

1. Log into the NetBlazer on your administrator's workstation and enter the **AppleTalk Interface** menu.

2. The first interface you establish becomes the default interface. Use the **appletalk interface add** <interface> nonroute|nonseed|<net> [-<net>] <zone> command to establish the default interface. If nonseed or nonroute operation is indicated, omit the network number(s) and zone strings.

   The example below establishes en0 as the default interface with a network number of 100 containing three zones (Marketing, Finance, and Admin).

```
NB:Top>Configure>AppleTalk>Interface> add en0 100 Marketing Finance Admin
AppleTalk Info #333 in RegisterOurName(900): Registered name "opal" on port 0.
AppleTalk port #0 assigned to interface 'en0'
Interface 'en0' has been designated as the default AppleTalk port.
NB:Top>Configure>AppleTalk>Interface>
```

Note: *If you use spaces or special characters in the zone, you must surround them with double quotes (i.e., "The Zone") so that the NetBlazer sees the string as one argument. Not doing so causes the NetBlazer to create a separate zone for each text string separated by a space (i.e., "The" and "Zone").*

3. If you intend to use the NetBlazer as a local router, repeat Step 2 for the remaining Ethernet interface(s).

4. Verify the interface information entered by reviewing it using the **appletalk interface list** command.

```
NB:Top>Configure>AppleTalk>Interface> list
port #  name      network range  zones
------  --------  -------------  ----------------------------------------
*   0   en0         100          Marketing Finance Admin
NB:Top>Configure>AppleTalk>Interface>
```

   If you need to make corrections, use the **appletalk interface delete** command and repeat Step 2.

5. Save the configuration by entering the **save** command.

The NetBlazer uses dynamic links to establish packet mode (PPP) AppleTalk connections between local and remote sites. You may use either dial-up asynchronous lines, V.25*bis* ISDN, or Switched-56 synchronous interfaces to create these connections.

The following steps describe the basic procedure for configuring dynamic links. For additional information, refer to Chapter 2, NetBlazer Interface Descriptions.

Asynchronous Dynamic Link

To establish a dial-up asynchronous connection, begin by entering the Interface Dynamic menu on the NetBlazer, then specifying **pppdial**:

```
opal:Top>Configure>Interface>Dynamic> pppdial
Name of the remote (other) system: jade
Phone number: 408 555-1720
Authentication method (crypto, password, none) [c]: password
Password to send to remote system (no echo):
Re-enter the password:
Add dialout 'jade'
Add user 'jade'
Add dynamic interface=jade, user=opal chat=ics, without crypto handshaking
 using PPP, MRU=1500
Okay (yes|no|quit) [y]? y
REMINDER! You need to set up route(s) for this interface
opal:Top>Configure>Interface>Dynamic>
```

1. Enter the name of the remote host at the first prompt.
2. The next prompt asks for the telephone number of the remote host. Enter this number. (Spaces and hyphens within the telephone number are permitted as long as the modem being used allows them in the dial string).
3. Enter the authentication method desired.
4. Review your entries and confirm by indicating **y** at the Okay prompt.
5. Enter the AppleTalk Interface menu and add the remote host name:

```
opal:Top>Configure>AppleTalk>Interface> add jade
AppleTalk port #4 assigned to interface 'jade'
opal:Top>Configure>AppleTalk>Interface>
```

6. Enter static routes using the **appletalk route add** command, or issue the **appletalk route learn** command on each end to learn the zones within the network to which each NetBlazer is connected.
7. Save the configuration by entering the **save** command.

8. Steps 1 through 7 must be also be performed on the remote NetBlazer.

Synchronous Links

A synchronous link may be either dedicated, as is the case in a leased-line situation, or a dynamic switched connection, as in an ISDN or Switched-56 connection.

Dedicated Synchronous Link

To establish a dedicated synchronous link over a leased line, you must be sure your data service unit/channel switching units (DSU/CSUs) are active and linked. The NetBlazer configuration procedure involves five basic steps:

1. Using the **interface attach** command to attach the line to the desired device (e.g., syn0, syn01, syn03, etc.), specify PPP and name the interface (e.g., sync-Atlanta).

2. Use the **appletalk interface add** command to bind AppleTalk and the interface name to the synchronous line.

Note: *Once this line is dedicated, it is not available for dynamic or dial-out use.*

```
opal:Top>Configure>Line> interface
opal:Top>Configure>Interface> attach syn0 ppp sync-atlanta
syn0: interface=sync-atlanta, protocol=PPP, MRU=1500, ip
address=143.191.64.17
opal:Top>Configure>Interface> appletalk interface
opal:Top>Configure>AppleTalk>Interface> add sync-atlanta
AppleTalk port #1 assigned to interface 'sync-atlanta'
```

3. Repeat steps 1 through 3 on the remote NetBlazer and save the configuration.

4. If you do not enter static routes, issue the **appleTalk route learn** command on each end to learn the zones within the network to which each NetBlazer is connected.

5. Save the configuration by entering the **save** command.

Additional details of this procedure are described in Chapter 2, NetBlazer Interface Descriptions.

Dynamic Backup of a Synchronous Link

The NetBlazer allows you to implement a dynamic (dial-up) backup of a dedicated synchronous link between two NetBlazers in case the leased line goes down. If this happens, packets are automatically forwarded to their destination over a dynamic asynchronous line. Refer to page 2-6 for an overview on configuring this facility.

This type of link uses the synchronous line to perform dialing. Although normally the synchronous interface is used on a dedicated leased line with CSU/DSUs, you can also use it with Switched-56 and ISDN services. These services provide dial-up capability, which is supported through the NetBlazer's V.25*bis* dialing function under the Line menu. Refer to page 2-11 for an overview on configuring this facility.

ARA Configuration

To set up the NetBlazer as an ARA server, you must first complete steps 1 through 4 in the Configuring the NetBlazer's Ethernet Port section (page 16-5).

1. With your list of user information at hand, use the **user add** command to add each remote user. This command prompts for all required information.

```
NetBlazer:Top>Configure>User> add
Enter the uname (1-32 chars): Heronomus
What kind of user (character, SLIP, PPP, ARA, ACS): ARA
The passwords of ARA users are stored as crypto keys.
Enter the crypto key (no echo):
Re-enter the crypto key:
Enter the callback telephone number [none]:
Enter the time limit [unlimited]:
Enter the user's home zone [none]: Marketing
User: Heronomus          privs:          B  dest-group:
Okay (yes|no|quit) [y]? y
NetBlazer:Top>Configure>User>
```

User Names and Passwords

2. Enter ARA user names. Names entered in response to the "Enter uname" prompt can be up to 31 characters in length and include spaces and any other special characters consistent with Apple conventions.

3. Enter the user's password. Passwords can be up to 8 characters in length.

Tip: *ARA Passwords are stored in the NetBlazer crypto handshake field as clear text, because encrypted passwords are not supported by the ARA authentication algorithm. For this reason, you should ensure that ARA user passwords are maintained locally on the NetBlazer, and access to the NetBlazer's STARTUP.CNF file is controlled. You should also ensure that only "trusted" users can log in to the NetBlazer with system configuration privileges.*

Notes:

1. *When using the NetBlazer's command line to add or change users, spaces or special characters must be surrounded with double quotes for the NetBlazer to see the string as one argument. For example, enter the name J. Random User as* ***"J. Random User"****. (These quotes should* ***not*** *be used in the* ***user add*** *command).*

2. *When using the NetBlazer's* ***user crypto*** *command line to add or change passwords, if spaces or special characters are used within the password, you must surround them with double quotes in order for the NetBlazer to see the string as one argument.*

Callback

4. Remote users can have the NetBlazer automatically call them back as an additional security measure or to reverse toll charges. Enter **y** when prompted to activate this function. You are then asked to enter the callback number (spaces and hyphens within the telephone number are permitted as long as the modem being used allows them in the dial string).

5. If it is necessary to place a maximum time limit on the connection, enter the time limit in minutes. The default is no limit.

Note: *You may wish to advise your ARA users that in the event they have an ARA connection through the NetBlazer and your timeout value expires, they will receive a* "two minute warning" *message approximately two minutes before the NetBlazer closes the connection.*

6. If the user wishes to log into his or her home zone, enter **y** to the `Use home zone?` prompt and enter the name of the user's home zone at the next prompt.

7. Repeat steps 1 through 5 until you have entered all remote users.

8. Save your remote user entries by issuing the **save** command.

The following topics cover the steps involved in performing various additional functions you may wish to use.

Home Zone

When a remote user wishes to automatically appear in his or her home zone when calling in, use the **configure user homezone** command to assign the remote user to the desired home zone:

```
opal:Top>Configure>User> homezone gary finance
```

If an ARA user's home zone is not explicitly stated, the default is the NetBlazer's home zone. To remove a user's homezone once it has been set, use two double quotes with no space between them (a null string), i.e., **configure user homezone** <user> "".

Zone Filtering

Use the **zonefilter** command to establish the desired zone access for each remote user where zone restriction is necessary. Initially, remote users have access to all zones.

Using the **permit** command gives a specified user access to only specified zones, while the **deny** command restricts the user from the specified zones.

Note that a user's homezone is always permitted.

```
opal:Top>Configure>AppleTalk>Zonefilter> ?
Available commands:
deny            list            permit          top>
up>             ?
```

Guest Access

If you wish to provide remote guest access to your network, you need to use the **configure user add** command to create a user named ara-guest. To logon to the network, the remote ara guest clicks on the **Guest** dialog box on his or her Macintosh.

```
opal:Top>Configure>User> add
Enter the uname (1-32 chars): ara-guest
Enter the time limit [unlimited]:
Enter the user's home zone [none]: Marketing
User: ara-guest          privs:        B  dest-group:
Okay (yes|no|quit) [y]? y
```

Once the ara-guest user name is established, remote guests have access to any network services not requiring authentication (they log on as **guest**). By default, an ara guest is allowed access to any zone and/or device (i.e., printers) that does not require authentication. If a more robust level of security is desired, you will most likely want to restrict the zones to which guest access is allowed. In this case use the **appletalk zonefilter permit** or **deny** commands to protect sensitive zones.

Note that the callback and crypto prompts do not occur for ara-guest.

ADSP Server

An ADSP server is provided to permit Macintosh users who wish to use a communications package to log into the NetBlazer to perform configuration, or login to a remote host. The factory default is ADSP active. If you wish to turn the ADSP server off or back on:

1. Be sure the AppleTalk interface is active as described in the Configuring the NetBlazer's Ethernet Port section.

2. Enter the Servers Start menu:

```
opal:Top>Configure>Servers>Start> ?
Available commands:
adsp            bootpd          discard         echo
finger          ftp             gdb             list
raw             rip             snmp            ipxsnmp
status          top>            telnet          up>
watchdog        ?
```

3. Enter **adsp** to start the server.

4. To stop the ADSP server, perform steps 1 through 3 from the Servers Stop menu.

Maintenance Functions

The following tables are provided as a convenience in performing common maintenance functions.

ARA Users

Table 16-1. ARA User Maintenance

Function	Command Sequence
Change ARA user's password	configure user crypto
Delete an ARA user	configure user delete
Change an ARA user's callback number	configure dialout phone
Change an ARA user's home zone	configure user homezone

Dynamic PPP Links

Table 16-2. Dynamic PPP Link Maintenance

Function	Command Sequence
Changing a host telephone number	configure dialout phone
Change inactivity timeout	interface dynamic timeout
Add and delete static routes	appletalk route add/delete
Learn and Forget routes	appletalk route learn appletalk route forget

NetBlazer™

Appendices

NetBlazer File Definitions A

NetBlazer 2.0 files are furnished on two distribution diskettes: the System diskette, and a Utilities diskette. Customers wishing only to upgrade from version 1.5 to 2.0 without the AppleTalk and IPX protocols will receive a single diskette. The ACS option will be provided on a separate diskette.

The NetBlazer uses the following files on the System diskette (* indicates post configuration added files):

- **TELEBIT.SYS** – This is the operating system file that is used to load and execute the NetBlazer's executable code. This file must be the first file on the diskette for the NetBlazer to boot correctly.
- **BOOTP** – This is the executable file that is used to load the NetBlazer executable code from a bootp server instead of from a floppy disk.
- **CHAT.TXT** – This file controls the log-in and authentication exchange, which takes place between the NetBlazer and a remote device (usually another NetBlazer) when establishing a packet mode connection.
- **DEFAULT.CNF** – This file contains the default configuration commands set by Telebit. You can restore the NetBlazer to its default configuration by copying this file to the STARTUP.CNF file and rebooting the system.
- **FRED** – This file contains the NetBlazer's executable code that runs under TELEBIT.SYS.
- **MODEMCAP.TXT** – This file contains the modem capabilities definitions for modems that are supported by the NetBlazer. This information is used in conjunction with the dialout and line characteristics to automatically configure the modems attached to the NetBlazer.
- **PASSWD*** – The NetBlazer system software uses this file (when the NetBlazer is powered up or rebooted) to keep track of authorized user logins and permissions. This facilitates using UNIX password files to create or update the NetBlazer's list of authorized users.
- **STARTUP.CNF*** – This file contains configuration commands, which are loaded when the NetBlazer is powered up or rebooted. Issuing a **configure save** command updates the STARTUP.CNF file for the current configuration.
- **TOKEN002.MCD** – This file contains the executable microcode for the Token Ring board that is down loaded to the Token Ring Board on startup.

Another group of files on the system diskette are the loader (.LDR) files. These files are automatically loaded when a command is issued that calls for the required overlay. Once loaded, these overlays remain resident in the NetBlazer's system memory until the NetBlazer is rebooted. Loader files furnished on the System diskette include:

- **ATK.LDR** – AppleTalk loader file. This overlay contains the extension that supports the NetBlazers AppleTalk protocol.
- **EDIT.LDR** – The file is the overlay for the NetBlazer's **edit** command.
- **IPX.LDR** – IPX loader file. This overlay contains the extension that supports the NetBlazers IPX protocol.
- **SNMP.LDR** – The SNMP loader file. This overlay contains the extension that supports the NetBlazers SNMP protocol.
- **TCL.LDR** – The TCL loader file. TCL (Tool Command Language – pronounced "tickle") is a tool provided to advanced users as a convenience in writing NetBlazer command scripts.

The second NetBlazer distribution diskette is the Utilities diskette. With the exception of the MIB.TXT file, the files on this diskette support the IPX remote shell program. The following files are included:

- **COMPPP.EXE** – This is the program that provides the PPP protocol and the serial port driver.
- **IPX.COM** – This file is actually two-part program. The top half is IPX and SPX from Novell. The bottom half are link programs that talk to the PPP driver.
- **IPXPPP.LAN** – This file includes the LAN driver (the LAN driver allows IPX to operate over an asynchronous PPP serial link). Novell's workstation generation program, WSGEN, uses IPXPPP.LAN and a Novell file to produce an IPX.COM program. Because Telebit provides a linked IPX.COM program with the NetBlazer, most customers do not need to execute WSGEN.
- **PPPCFG.EXE** – This file is the PPP Configuration and Management program.
- **PPPCFG.HLP** – This is the Help extension file for the PPP Configuration program.
- **PPPCFG.MDM** – This is the modem configuration file for PPPCFG.EXE program.
- **WATCHPPP.EXE** – This file is a TSR (Terminate Stay Resident) program that warns of attempts to access large executable programs. This warning reminds the user when attempting to download a large file over the serial link that may take several minutes, and offers the chance to abort.

- **MIB.TXT** – This file is the Telebit Enterprise MIB text, which was developed to provide extended NetBlazer configurability over the provisions of MIB-II. This file is compatible with most MIB compilers in applications where the NetBlazer is to be managed by a Network Management Station.
- **MIB.CMU** – This file is also the Telebit Enterprise MIB text, but provided for compatibility with the popular Carnegie Mellon University MIB compiler tools.

Editing a NetBlazer File Using MS-DOS

Although the NetBlazer does not run under MS-DOS, its diskette and file formats are compatible with MS-DOS. Therefore, you can edit any of the configuration (CNF) or text (TXT) files on the NetBlazer diskette using a text editor program on any MS-DOS computer system that supports high density 1.44 Mbyte 3.5 inch diskettes.

You should make a duplicate copy of the NetBlazer system diskette using the DISKCOPY command on your DOS system. Use the duplicate diskette as a working copy, and put the original NetBlazer system diskette in a safe place.

STARTUP.CNF File Definition

The NetBlazer STARTUP.CNF file consists of a list of NetBlazer commands that are executed in sequence each time the NetBlazer is powered up or rebooted. Refer to the *NetBlazer Command Reference Manual*, for a description of the commands used by the NetBlazer.

When editing the STARTUP.CNF file, do not use commands such as **ipdial** that require operator input, and include all required parameters in each command entered. Also avoid using commands that may have adverse or unpredictable results such as **reboot**, **save** or any of the **disk** commands.

Pay special attention to the order in which the configuration commands are entered. Since the commands are executed in sequence starting at the top and working down through the file, configuration commands that define parameters used by other commands should be entered earlier in the list. Several cases where the command order is important are listed below.

- The IP address must be set before any command is entered that would cause the NetBlazer to start transmitting IP packets.
- Commands defining the NetBlazer interfaces should be entered before commands used to specify routes.

- Commands used to create and define a characteristics group should be entered before any command that requires a group name as one of its parameters.

Also keep in mind that a command appearing later in the list may override an earlier command.

NetBlazer PASSWD File

The NetBlazer uses a PASSWD file to keep track of authorized user logins and permissions. The record format of the NetBlazer's PASSWD file, shown in Figure A-1, is similar to the password file format used by UNIX. This allows you to download user records from a UNIX password file on a remote host.

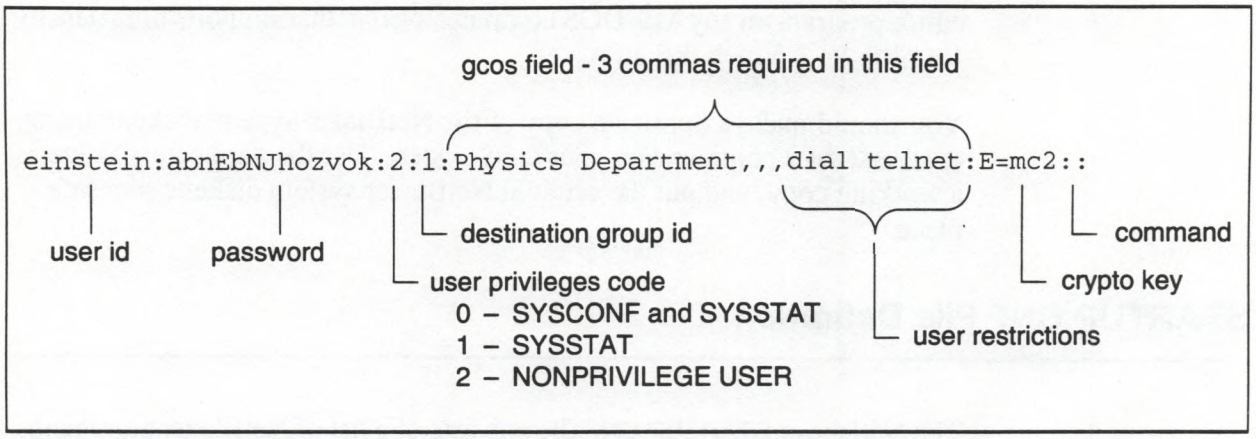


Figure A-1. NetBlazer PASSWD File Record Format

Like the password file format used by UNIX, each record in the NetBlazer PASSWD file consists of seven fields separated by colons. However, the definitions of the fields used in the NetBlazer and UNIX password files differ as shown in Table A-1.

Table A-1. Password File Field Definitions

Field	UNIX Password File	NetBlazer Password File
1	userid – user's login name	userid – user's login name
2	password – user's encrypted password	password – user's encrypted password
3	uid – user's ID number	user's numeric privileges code (0,1, or 2)

Note: If the gcos field in a UNIX password file contains three or more commas, the NetBlazer treats the record as a NetBlazer record. To prevent misinterpreting fields 6 and 7, the NetBlazer discards an entry in either of these two fields that begins with a slash (/).

Colons (:) are used as field separates in the password records and are not allowed in the fields.

Table A-1. Password File Field Definitions

Field	UNIX Password File	NetBlazer Password File
4	gid – user's group ID number	user's destination group ID number
5	gcos field – information about the user	gcos field and user restrictions – see note
6	home dir – user's home directory	crypto key – used for packet mode connections
7	login shell – user's initial shell program	login command – executed when user logs in.

Note: If the gcos field in a UNIX password file contains three or more commas, the NetBlazer treats the record as a NetBlazer record. To prevent misinterpreting fields 6 and 7, the NetBlazer discards an entry in either of these two fields that begins with a slash (/).

Colons (:) are used as field separates in the password records and are not allowed in the fields.

The **userid** field is the user's login name. This field must contain from 1 to 32 characters.

The **password** field is the user's encrypted password. If this field is empty, a password is not required for that user to log in.

The **user privileges code** field determines whether or not the user has system configuration or status privileges. Only system administrators should be granted system configuration or status privileges (privilege codes 0 or 1). If this field contains a value of 2 or greater, the user is assigned nonprivilege user status (privilege code 2).

The **destination group id** field is the gid number of the destination group assigned to the user. If this field's value does not point to a destination group with a matching gid number, the field is left empty, indicating that the user does not have an assigned destination group.

The **gcos** field in a NetBlazer PASSWD record must always contain three commas. This divides the field into four parts. The first three parts contain information about the user taken from the UNIX password file. The last part, **user restrictions**, indicates if the user's dial-out and/or telnet privileges are restricted to the user's assigned destination group.

The **crypto key** normally is used during a crypto handshaking sequence to authenticate a packet mode connection. This field should be blank for login users unless they have some way to generate the correct responses to a crypto challenge. For a packet mode connection between two NetBlazers, the crypto key assigned to the dynamic interface on the calling NetBlazer must match the crypto key assigned to the corresponding user record on the answering NetBlazer.

The **command** field is used to enter a string of NetBlazer commands that will automatically execute when the user logs in. Semicolons are used as separators between commands.

Editing a Copy of the UNIX Password File

If you choose to edit a copy of the UNIX password file before transferring it to the NetBlazer, you should observe the following guidelines:

- Make sure that you are using a copy of the master password file, which includes the encrypted passwords.
- Records with an asterisk (*) in the first character position of the **password** field are skipped by the NetBlazer when loading the password file.
- Records that do not contain at least three commas in the **gcos** field are treated as UNIX password records. In such a case, only the **userid**, **password**, and **gcos** fields are used. The remaining fields are set to the default values listed in Table A-2.

Table A-2. NetBlazer PASSWD File Default Values

Field	NetBlazer Field Name	Default Value
1	userid	UNIX user's login name
2	password	UNIX user's encrypted password
3	user's privileges code	2 – nonprivileged user
4	user's destination group ID number	null – no destination group assigned
5	gcos field and user restrictions	UNIX user's gcos information, no restrictions
6	crypto key	null – no crypto key
7	command	null – no login command

The remaining guidelines in this section only apply to NetBlazer records, which include at least three commas in the **gcos** field. All other records are treated as a UNIX password file as described earlier.

- Any **user restrictions** (i.e. dial and/or telnet) must follow the last comma in the **gcos** field. If you do not want to restrict a user's dial-out or telnet privileges to the user's assigned destination group, the third comma should be the last character in the **gcos** field.
- Users with a **uid** equal to 2 or greater are assigned nonprivileged user status by the NetBlazer. Therefore, you do not need to change the **uid** field for most UNIX users, unless you want to grant a user NetBlazer system configuration and/or status privileges.
- If a user's **destination group ID** field does not point to a destination group with a matching gid number when the password file is loaded, it is replaced by a null value indicating that the user does not have an assigned destination group.
- To make sure that a group of users are assigned to the proper destination group, you can either edit the users' **destination group ID** fields to point to an existing destination group, or create a destination group on the NetBlazer with a gid number that matches the users' **destination group ID** field. See Setting Up User Destination Groups on page 11-4.
- To prevent misinterpreting the UNIX **home dir** field as a **crypto key**, the NetBlazer discards entries in the **crypto key** field that begin with a slash (/). Therefore, you should not need to change the **crypto key** fields because normal users typically do not use crypto handshaking when logging in to the NetBlazer.
- Entries with a slash (/) in the **command** field are set to null.

Loading a Password File into the NetBlazer

Before loading a password file into the NetBlazer, make sure that you understand how the NetBlazer will treat each record in the password file by reading Editing a Copy of the UNIX Password File on page A-6.

If you want a group of users to be automatically assigned to a particular destination group, make sure that a destination group with a matching gid number exists. For instructions on how to create a destination group, refer to Setting Up User Destination Groups in Chapter 11.

Caution: *When a password file is loaded into the NetBlazer, the user records in the password file overwrite any current user records that have userids that are identical to the password file's userids.*

Refer to the **user load** command description in the *NetBlazer Command Reference Manual* for details on downloading user information from a password file into the NetBlazer.

For instructions on how to configure the NetBlazer to access a remote password file over the network, see Chapter 14, Network Management.

MODEMCAP.TXT File Definition

The MODEMCAP.TXT file contains definitions of the various Telebit modems supported by the NetBlazer. You can edit the MODEMCAP.TXT file to add support for modem features that are not already supported.

When the NetBlazer detects an off-to-on transition on the DSR line of a RS-232 port, it attempts to determine the type of modem attached to that port by sending ATI and AT~I commands and checking the numeric product identification code. The NetBlazer use the modem's response to select a modemcap entry in the MODEMCAP.TXT file. If the NetBlazer does not receive a response or if it does not find a matching code in the MODEMCAP.TXT file, the NetBlazer assumes that there is no modem attached to the line and starts a standard terminal login on that line.

Command Line Formats

The MODEMCAP.TXT file is composed of a series of command lines. The following four basic types of command lines are used:

- A **label** is any alphanumeric string starting at the left-most character position in the line. It denotes the beginning of a new modem definition. The modem definition continues until another label is encountered in the command line sequence.

- A **tag** is always preceded by white space, i.e. a number of spaces or tab characters, and consists of a tag name followed by a colon (:) and the value assigned to that tag. In many cases, the value assigned to a tag is a modem command string. Refer to your modem's reference manual for descriptions of the modem commands and registers.
- The **$include:<label>** metacommand is used to include a previous definition in the current modem definition. Like the tag command line, a $include command line must be preceded by white space.
- A **comment** line is any line that has a pound character (#) in the first character position. It is used to add descriptive information to the MODEMCAP.TXT file.

The character sequences defined in Table A-3 may be used in a tag command line to perform special functions.

Table A-3. Special Functions Character Sequence

Character Sequence	Description
\b	send a backspace character
\f	send a formfeed character
\n	send a newline character (linefeed)
\r	send a carriage return character
\t	send a tab character
\\	send a backslash character
\?	send a question mark character
\'	send a single quote character
\"	send a double quote character
\0	send the null character (value zero)
\ooo	send the character whose value is the three octal digits following the backslash
\xhh	send the character whose value is the two hexadecimal digits following the backslash and the letter "x"

Required Tag Commands

The command line tags defined in Table 1-4 are required in each modem type definition along with the modem identification string that is returned in response to ATI and AT~I modem identification commands. These tags are provided to allow non-Telebit modem to recognize NetBlazer issued modem commands, and modem responses to be recognized by the NetBlazer.

Table 1-4. Required Tag Commands

Tag	Definition	Type
dial	string that precedes phone number	command
hard-reset[0-3]	strings used to initialize modem	command
reset-pause	milliseconds to pause after resetting modem	command
speed-cmd	command to set modem speed while using modem	command
line-speed	NetBlazer line speed while using modem	command
autospeed-cmd	command to set modem speed while configuring modem	command
autospeed	NetBlazer line speed while configuring modem	command
list-cmd	command to display the current modem configuration	command
line-characteristics	characteristic used to match dialout's characteristics	command
no-answer	string to turn off answering (e.g. ats0=0)	command
write-cmd	string to write configuration to NVRAM (e.g. AT&W)	command
result-ok	ok result codes (a comma separated list)	response
result-fail	failure result codes	response
result-busy	busy result codes	response
result-ignore	ignored result codes	response
result-noanswer	noanswer result codes	response
result-nocarrier	no carrier result codes	response
result-nodial	no dial tone result codes	response
at-cmd	autobaud recognition sequence (defaults to AT)	command
no-echo	autobaud and turn off echo (defaults to ATE0)	command

Dial Tag

As illustrated below, the **dial** tag defines the modem command that is sent by the NetBlazer when dialing out to a remote location.

```
dial:atdt %s
```

The NetBlazer dialout code replaces the %s with the actual phone number when dialing takes place.

Hard-Reset Tag

The **hard-reset** tags specify the modem command strings that are sent to the modem when the NetBlazer determines that the modem is not properly configured. A modem definition may include from one to four hard-reset command lines, labeled **hard-reset0** through **hard-reset3**.

Here are the **hard-reset** tags for the Telebit T2500 modem:

```
hard-reset0:at~&fs51=254e0v0x14s0=1s2=128s45=255s50=0s52=2s54=3s55=3s58=2s131=1
hard-reset1:ats64=1s66=1s68=2s92=1s95=2s97=1s98=3s106=1s130=0
```

When resetting a modem, the NetBlazer issues each modem command string in sequence.

Reset-pause Tag

The **reset-pause** tag specifies the amount of time in milliseconds that the NetBlazer should wait before getting the active configuration after using the **hard-reset** tags to reconfigure the modem.

```
reset-pause:200
```

Speed-cmd and Line-speed Tag

The **speed-cmd** and **line-speed** tags are used to synchronize the interface speed of the modem to the interface speed of the NetBlazer while using the modem.

```
speed-cmd:ats51=5
line-speed:19200
```

Autospeed-cmd and Autospeed Tags

The **autospeed-cmd** and **autospeed** tags are used to synchronize the interface speed of the modem to the interface speed of the NetBlazer while configuring the modem.

```
autospeed-cmd:ats51=254
autospeed:19200
```

List-cmd Tag

The **list-cmd** tag specifies the modem command that is used to get the current configuration of the modem. The NetBlazer uses this information to determine if the modem's active configuration has been changed by performing a hard reset. If the modem's active configuration following a hard reset differs from its configuration prior to the hard reset, the NetBlazer writes the active configuration in the modem's non-volatile memory.

```
list-cmd:at~n?
```

Line-Characteristics Tag

The **line-characteristics** tag specifies the default characteristics group that is assigned to any line attached to the defined type of modem. The following is the standard entry that is preassigned for all Telebit modems:

```
line-characteristics:dialout
```

Note that this default characteristics group can be overruled on a line-by-line basis by issuing a **line characteristics** command for a specified line and saving the current configuration by issuing a **configure save** command.

No-answer Tag

The **no-answer** tag defines the modem command that is used to prevent the modem from answering incoming calls.

```
no-answer:ats0=0
```

Write-cmd Tag

This command is used to modify or store new modem power-on startup parameters in the modem's non-volatile RAM. Telebit modems use the syntax AT&W.

Result-ok Tag

The **result-ok** tag defines the identification code that is returned by the modem to indicate it has accepted your command, or it has completed the connection. S = ok = result-ok = 0, 1, 5, 10-14, 20, 22-25, 30-39, 46-48, 50, 61-63, 70-73.

A "0" response indicates the modem has successfully accepted your command or established connection. The remaining codes are connect codes.

Result-fail Tag

The **result-fail** tag defines the identification code that is returned by the modem to indicate it has failed to accepted your command.

F = fail = result-fail. All undefined values are considered a failure. These include 4 (call failure). Thus 2, 4, 9, 15-19, 21, 26-29, 40-45, 49, 51-60, 64-69, and 74- are all considered call failure.

Result-busy Tag

The **result-busy** tag defines the identification code that is returned by the modem to indicate the number called is busy. B = busy = result-busy = 7.

Result-ignore Tag

The **result-ignore** tag exists because sometimes the modem presents a stray "ring" message to the NetBlazer while the NetBlazer is waiting for the modem to respond to a command the NetBlazer has sent to the modem. I = ignore = result-ignore = 52,53.

Result-noanswer Tag

The **result-noanswer** tag defines the identification code that is returned by the modem to indicate the number called was not answered. N = noanswer = result-noanswer = 8.

Result-nocarrier Tag

The **result-nocarrier** tag defines the identification code that is returned by the modem to indicate it did not receive a carrier (no DCD). C = nocarrier = result-nocarrier = 3.

Result-nodial Tag

The **result-nodial** tag defines the identification code that is returned by the modem to indicate it did not receive a dial tone. D = nodial = result-nodial = 6.

At-cmd Tag

The **at-cmd** tag defines the modem command that your particular modem recognizes as the "AT" command. "at-cmd" = "AT".

No-echo Tag

The **no-echo** tag defines the modem command that is used to set the modem to suspend echoed characters. "no-echo" = "ATE0".

Modem ID Response Tag

The last mandatory tag is the identification code that is returned by the modem in response to the AT~I command. Usually there are two codes, one that will be returned by the modem when it has been properly preconfigured (does not require a hard-reset string) and one that indicates that it is not preconfigured and must be reset.

For example, the T2500 modem uses the following modem ID response tags:

```
971:0
9710:1
972:0
9720:1
```

Since the NetBlazer uses the numeric response mode of the modem and the modem normally generates text response codes, this is used by the NetBlazer to indicate whether or not the modem is configured. These tags are special in that the name of the tag is the code that is returned in response to the ATI and AT~I commands The value is either 0 (the NetBlazer should send the hard-reset string to the modem) or 1 (the modem is preconfigured).

Specific Function Tags

Several tags included in the MODEMCAP.TXT file enable or disable a particular modem function.

Table 1-5. Special Function Tag Commands

Characteristic Tag	Definition
pep	string to put the modem into PEP mode
v32	string to put the modem into v32 mode
nov42	string to turn off v42 mode
nov42bis	string to turn off v42bis mode
mnpoff	string to turn off mnp compression
bell212a	string to put the modem into bell212a mode
sane	string to put the modem into human-friendly mode
ara-bs	string to turn on ARA byte swapping
The following two tags are used together for modems that do not hang up the line when DTR is lowered.	
attention	usual "+++" in pause +++ pause attention sequence
hang-up	hang up command

Refer to Using Characteristics Groups in Chapter 10 for a description of how to use these function tags to select and preconfigure a modem when dialing out to a remote system.

The sane tag is used for modem pooling when you wish to put the modem into a "human-friendly" mode with more verbose result codes and echo enabled.

The ara-bs tag supports the Apple "byte swap" modification to for AppleTalk ARA negotiation of v.42bis dictionary size. This tag tells the NetBlazer to configure the modem to support AppleTalk ARA.

Creating New Function Tags

If you need to control a particular function of a modem that does not have a defined function tag in the MODEMCAP.TXT file, you can add your own function tag and associated modem commands to one or more of the modem definitions contained in the MODEMCAP.TXT file. However, if you are not quite sure how to proceed, contact your technical support representative for assistance.

Using The Debug Modemcap Command

The **debug modemcap** <modem> command displays the modem entries that currently exist in your MODEMCAP.TXT file.

If you do not specify a <modem>, a list of possible entries is displayed. This is particularly useful when you need to know the correct syntax for the modem type.

Modem MIB Support Tags

Several tags are included in the MODEMCAP.TXT file to provide support for the management of modems using SNMP. Tags that are preceded with "query" define an actual command that will be sent to the modem and, as such, should only be defined if the modem supports such a command. The remaining tags help to identify a modem, and are never used as modem commands.

Table 1-6. MIB Support Tags

Characteristic Tag	Definition
manufacturer	string that is the builder of the modem
equip-type	string description of modem's equipment type 'sa' standalone, 'rm' rackmount, 'bi' built-in.
query-id	command to query modem for 'extended' ID, i.e., the modem's name/model & rev level.
query-lq	command to query modem for line quality.
query-cf	command to query modem for speed as configured.

The CHAT.TXT file automatically controls the conversation that takes place between the NetBlazer and a remote NetBlazer (or some other device) when attempting to establish a packet mode connection to exchange IP datagrams. This file uses a special programming language called chat script, which allows the NetBlazer to respond correctly to prompts from the remote system.

The CHAT.TXT file may include multiple chat scripts to allow the NetBlazer to call and establish a packet mode connection with different types of systems. Each chat script starts with a label that consists of colon (:) immediately followed by the chat script name. For example, :ics is the label assigned to the chat script used to control the log-in exchange between two NetBlazers.

Chat Script Commands

Generally, each command line in a chat script starts with a command letter and a state number followed by the command parameters, which are separated by commas. Any of the following chat script commands may be used:

send **s<num>,<tmo>,<tmo-st>,<next-st>,<string to send>**

This command allows the NetBlazer to send a character string to the remote system.

The <num> parameter is the state number of this command.

The <tmo> parameter is the timeout value in seconds.

The <tmo-st> parameter is the next state number if there was a timeout.

The <next-st> parameter is the next state number if the send was successful with no timeout.

The <string to send> parameter is the string to be sent to the remote system.

expect **e<num>,<tmo>,<tmo-st>,<next-st>,<string to expect>**
Expect-case **E<num>,<tmo>,<tmo-st>,<next-st>,<string to expect>**

These commands cause the NetBlazer to stop and wait for a string of characters from the remote system. The **expect** command is not case sensitive, whereas the **Expect-case** is case sensitive and the characters received must exactly match the <string to expect> parameter.

The <num> parameter is the state number of this command.

The <tmo> parameter is the timeout value in seconds.

The <tmo-st> parameter is the next state if there was a timeout.

The <next-st> parameter is the next state if the expected string was received prior to timing out.

The <string to expect> parameter is the string to wait for from the remote system.

or **o<next-st>,<string to expect>**
Or-case **O<next-st>,<string to expect>**

These commands must immediately follow an **expect**, **Expect-case**, **or**, or **Or-case** command. This is how the NetBlazer can respond to one of several different expected strings and process them appropriately. The **or** command is not case sensitive, whereas the **Or-case** is case sensitive and the characters received must exactly match <string to expect>.

The <next-st> parameter is the next state if the expected string was received prior to timing out

The <string to expect> parameter is the string to wait for from the remote system.

return **r<num>,<ret-val>**

This command is the end state for a chat script. It returns a value that indicates the success or failure of the connection.

The <num> parameter is the state number of this command.

A <ret-val> of zero (0) indicates that the chat was successful and that packet mode is enabled remotely. A non-zero <ret-val> indicates failure.

uname **u<num>,<tmo>,<tmo-st>,<next-st>**
password **p<num>,<tmo>,<tmo-st>,<next-st>**

The **uname** and **password** commands are how the chat script transmits the user name and password. Unlike the **send** command, which always transmits the same string, these commands get the string to send from the interface information.

The <num> parameter is the state number of this command.

The <tmo> parameter is the timeout value in seconds.

The <tmo-st> parameter is the next state if there was a timeout.

The <next-st> parameter is the next state if the expected string was received prior to timing out.

get-challenge **c<num>,<tmo>,<tmo-st>,<next-st>**

The **get-challenge** command reads the crypto challenge from the remote system. Usually control is transferred to this state after a successful expect of "challenge." This command reads the crypto challenge and feeds it into the crypto challenge processing code where a response is generated. The next state is almost always a **send response** command.

The <num> parameter is the state number of this command.

The <tmo> parameter is the timeout value in seconds.

The <tmo-st> parameter is the next state if there was a timeout.

The <next-st> parameter is the next state if the challenge was received prior to timing out.

send-response **y<num>,<tmo>,<tmo-st>,<next-st>**

The send-response command is used to transmit a response to a crypto challenge. This command always follows a get-challenge command.

The <num> parameter is the state number of this command.

The <tmo> parameter is the timeout value in seconds.

The <tmo-st> parameter is the next state if there was a timeout.

The <next-st> parameter is the next state if the challenge response was sent prior to timing out.

Chat Script Examples

The simplest chat script is one that immediately returns a success code. This would be used when a NetBlazer must call a system that does not require a login chat sequence (the called system has SLIP or PPP already running on the port and will never prompt for a user ID or a password). Here is such a script:

```
:null
r1,0
```

A more complex chat script is the ics chat script used by the NetBlazer to establish a packet mode connection with another NetBlazer.

```
:ics
e1,10,30,2,login:
```

Start the ics chat script and wait 10 seconds for a "login:" prompt from the remote NetBlazer. If the prompt is received, transition to state 2. If 10 seconds expire without receiving the login prompt, go to state 30.

```
u2,5,100,3
s3,5,100,4,\r
```

Send the user ID and a carriage return (\r) to the remote NetBlazer.

```
e4,5,30,5,password:
p5,5,100,6
s6,5,100,7,\r
```

Wait 5 seconds for a "password:" prompt. If 5 seconds expire without receiving the password prompt, go to state 30. If the prompt is received, send the password followed by a carriage return to the remote NetBlazer.

```
e7,5,30,99,Packet mode enabled
o32,login:
o20,challenge:
```

Wait 5 seconds for a string from the remote NetBlazer. If 5 seconds expire without receiving a string go to state 30. If a "Packet mode enabled" string is received, the login was successful; go to state 99. If a "login:" prompt is received, go to state 32. If a "challenge:" prompt is received, a crypto challenge is pending, go to state 20.

```
c20,5,30,21
e21,5,30,22,response:
y22,5,100,23
s23,5,100,7,\r
```

Accept the crypto challenge, and respond to the "response:" prompt by sending back the proper crypto response. Then, go back to state 7, and check for a "Packet mode enabled" string from the remote NetBlazer.

```
s30,5,100,31,\r\r
e31,10,100,32,login:
u32,5,100,33
s33,5,100,34,\r
e34,5,100,35,password:
p35,5,100,36
s36,5,100,37,\r
e37,5,100,99,Packet mode enabled
o100,login:
o50,challenge:
c50,5,100,51
e51,5,100,52,response:
y52,5,100,53
s53,5,100,37,\r
```

Something went wrong in the login process. Try sending a couple of carriage returns and repeat the whole process again. If unsuccessful this time, go to state 100 and return a failure code.

```
r99,0
r100,1
```

State 99 returns a success code indicating that the NetBlazer has successful established a packet mode connection with the remote NetBlazer; whereas state 100 returns a failure code indicating that something went wrong during the login sequence.

Telebit Enterprise MIB

System Administrators wishing to directly access the Telebit enterprise MIB using their SNMP network management software are directed to the text files embedded in the Telebit enterprise MIB. This file is on the Utility distribution diskette, and is heavily commented to provide adequate information for persons knowledgable in integrating managed object MIBs into network management applications.

Line Assignments B

Synchronous Lines

The line number for the NS1 single-port synchronous board is syn0. Line pairs from the SYNxxx dual-port synchronous boards have the numbers shown in Table B-1.

Table B-1. Dual-Port Synchronous Boards and Lines

Line Pairs	Switch Setting (SW2)
syn10, syn11	0
syn20, syn21	2
syn30, syn31	4
syn40, syn41	6
syn50, syn51	8

Asynchronous Lines

The asynchronous lines are identified with their associated boards in Table B-2 and Table B-3.

Also refer to the NetBlazer Option Boards Installation section in the *NetBlazer Installation Guide* for more information.

Table B-2. Internal Asynchronous Port Line Numbers

Line Number	Location	Port
00	First 16550	ASY00
01	Second 16550	ASY01
02	First 16450 (for NetBlazers ST and 40)	Console (ASY02)

Table B-3. Multi-Port Asynchronous Line Numbers

Line Number	Location	Port	Line Number	Location	Port
10	First NM8 board	1	104	ASYN8 board, MTA0	5
11	First NM8 board	2	105	ASYN8 board, MTA0	6
12	First NM8 board	3	106	ASYN8 board, MTA0	7
13	First NM8 board	4	107	ASYN8 board, MTA0	8
14	First NM8 board	5	110	ASYN8 board, MTA1	1
15	First NM8 board	6	111	ASYN8 board, MTA1	2
16	First NM8 board	7	112	ASYN8 board, MTA1	3
17	First NM8 board	8	113	ASYN8 board, MTA1	4
20	Second NM8 board	1	114	ASYN8 board, MTA1	5
21	Second NM8 board	2	115	ASYN8 board, MTA1	6
22	Second NM8 board	3	116	ASYN8 board, MTA1	7
23	Second NM8 board	4	117	ASYN8 board, MTA1	8
24	Second NM8 board	5	120	ASYN8 board, MTA2	1
25	Second NM8 board	6	121	ASYN8 board, MTA2	2
26	Second NM8 board	7	122	ASYN8 board, MTA2	3
27	Second NM8 board	8	123	ASYN8 board, MTA2	4
30	Third NM8 board	1	124	ASYN8 board, MTA2	5
31	Third NM8 board	2	125	ASYN8 board, MTA2	6
32	Third NM8 board	3	126	ASYN8 board, MTA2	7
33	Third NM8 board	4	127	ASYN8 board, MTA2	8
34	Third NM8 board	5	130	ASYN8 board, MTA3	1
35	Third NM8 board	6	131	ASYN8 board, MTA3	2
36	Third NM8 board	7	132	ASYN8 board, MTA3	3
37	Third NM8 board	8	133	ASYN8 board, MTA3	4
100	ASYN8 board, MTA0	1	134	ASYN8 board, MTA3	5
101	ASYN8 board, MTA0	2	135	ASYN8 board, MTA3	6
102	ASYN8 board, MTA0	3	136	ASYN8 board, MTA3	7
103	ASYN8 board, MTA0	4	137	ASYN8 board, MTA3	8

AppleTalk C-Style Octal Table

Ä \200	û \236	º \274
Å \201	ü \237	Ω \275
Ç \202	† \240	æ \276
É \203	° \241	ø \277
Ñ \204	¢ \242	¿ \300
Ö \205	£ \243	¡ \301
Ü \206	§ \244	¬ \302
á \207	• \245	√ \303
à \210	¶ \246	ƒ \304
â \211	ß \247	≈ \305
ä \212	® \250	Δ \306
ã \213	© \251	« \307
å \214	™ \252	» \310
ç \215	´ \253	… \311
é \216	¨ \254	\312
è \217	≠ \255	À \313
ê \220	Æ \256	Ã \314
ë \221	Ø \257	Õ \315
í \222	∞ \260	Œ \316
ì \223	± \261	œ \317
î \224	≤ \262	– \320
ï \225	≥ \263	— \321
ñ \226	¥ \264	“ \322
ó \227	µ \265	” \323
ò \230	∂ \266	‘ \324
ô \231	∑ \267	’ \325
ö \232	∏ \270	÷ \326
õ \233	π \271	◊ \327
ú \234	∫ \272	ÿ \330
ù \235	ª \273	

Index

A

ACS software option 1-5
address
  ARP broadcast 4-2
  global IP 4-2
  IP 4-1
address, peer IP 15-9
ADSP 3-6
ADSP server 16-1, 16-11
Apple Communications Toolbox 3-2, 3-6, 16-1
AppleTalk
  ADSP server 16-1, 16-11
  ARA callback 16-10
  ARA configuration, procedure 16-9
  ARA guest access 16-11
  ARA server 16-2
  ARA server, requirements 16-3
  ARA user homezone 16-10
  ARA user names 16-4
  ARA user passwords 16-4
  ARA user zone filtering 16-11
  ARA, operation 16-3
  configuration 16-1
  configuration preplanning 16-2
  configuring ethernet port 16-5
  C-style octal table C-1
  default settings 16-1
  dynamic link setup 16-7
  IP encapsulation in DDP 16-5
  learning zones 2-4
  maintenance functions 16-12
  network range, recommendations 16-2
  node startup range 16-2
  RTMP 16-3
  seed versus nonseed 16-3
  user names and passwords 16-9
  zone names 16-2
AppleTalk, route learn 16-5
ARA server 1-7, 16-2
ARP (see also proxy ARP) 8-1
ARP broadcast address 4-2
assigned port number 9-4
asynchronous lines B-1
ATK.LDR A-2
authentication 6-1
auto-route 7-1
auto-telnet 1-6

B

boot bootp command 14-3
booting UNIX host 14-1
BOOTP 14-3
  forwarding server 14-1
  overview 14-1
  server 14-3
bootptab field definitions 14-2

C

callback
  auto-telnet 12-1
  dial-out records 12-2
  packet mode 12-2
  request line, setup 12-1
  security, setup 12-1
CAPTURE.EXE 15-17
characteristic group 10-3
  assigning for raw or raw dial 13-1
  raw 13-1
characteristics 10-1
chat script A-16, A-18
CHAT.TXT A-16
command prompt 3-8
commands
  AppleTalk route learn 2-11
  AppleTalk, interface list 16-6
  AppleTalk, route learn 16-5
  boot bootp 14-3
  configure file 14-2
  file 14-4
  interface attach 2-4
  ip filter 9-1
  ipdial 5-3, 6-6
  ipx ping 15-15
  keepalive (IPX) 15-16
  line reset 13-2
  logout 3-10
  msglog 14-7

pppdial 2-9, 5-3, 15-11
save local 14-4
save remote 14-4
slipdial 2-9
syslog host 14-6
timeout (IPX keep-alive) 15-16
user command 11-8
user list 3-10
user remote 14-5
user userdomain 14-6
community groups, SNMP 14-8
community names 14-9
COMPPP.EXE 15-20, A-2
configuration
dedicated IP interface 5-1
IP 4-1
IPX 15-1
methods 3-2
testing IP 4-6
configure file 14-2
connection
dynamic dial-up 6-1
remote 6-1
crypto handshake 6-7, 6-9, 11-3
crypto key 6-1, 6-5, 6-9

D

date and time, setting 3-9
default filter 9-1
deny filter 9-1
destination group 11-1
destination unreachable, ICMP 9-1
dial-in record 6-7
dialout characteristics 10-5
dialout destination 10-1
dial-out records 6-8, 10-5, 12-2
dial-up router 1-2
DNS 14-6
domain name 4-6
dynamic (see interfaces, dynamic)
dynamic interfaces
AppleTalk routing 2-11
dial-in 2-8
dial-out 2-8
ip packet routing 2-10
ipx packet routing 2-11
overview 2-7
setup 2-8
values 2-9

E

EDIT.LDR A-2
enterprise MIB 14-9, A-20
enterprise MIB, access privileges 14-9
Ethernet 1-2

F

farside 6-11
file 14-4
file server 15-4, 15-6, 15-9, 15-16
FILER.EXE 15-17
files 11-1, 14-4
ATK.LDR A-2
CAPTURE.EXE 15-17
CHAT.TXT A-16
COMPPP.EXE 15-20, A-2
EDIT.LDR A-2
FILER.EXE 15-17
IPX.COM 15-20, A-2
IPX.LDR A-2
IPXPPP.LAN 15-17, A-2
LOGIN.EXE 15-17
LOGOUT.EXE 15-17
MAP.EXE 15-17
MIB.CMU A-3
MIB.TXT A-3
MODEMCAP.TXT A-8
NETX.COM 15-20
PASSWD A-4
password 14-4, 14-5
password, saving 3-11
PPPCFG.EXE 15-19, A-2
PPPCFG.HLP 15-17, A-2
PPPCFG.MDM A-2
SNMP.LDR A-2
STARTUP.CNF 3-1, 3-2, 3-5, A-3
SYSCON.EXE 15-17
TCL.LDR A-2
USERLIST.EXE 15-17
WATCHPPP.EXE 15-21, A-2
WHOAMI.EXE 15-17
FILES.CNF 14-4, 14-5
filtering, packet 9-1
flush 9-3
framing 5-2

framing, IPX 15-6
framing, ppp or slip (choosing) 2-10
FRED 14-3
functional overview 1-1

G

global address
IP 4-2

H

host name 15-3

I

ICMP destination unreachable 9-1
input filtering 9-1
interface 4-2
name 6-5
record 6-9
interface attach command 2-4
interface trace, using 14-7
interfaces
backup 5-2
dedicated 5-1
dedicated configurations 2-5
dedicated ppp, dynamic backup 2-6
descriptions 2-1
dynamic 6-4
dynamic AppleTalk packet routing 2-11
dynamic backup 5-2
dynamic IP 6-1
dynamic IPX 15-10
dynamic values 2-9
dynamic, dial-in 2-8
dynamic, dial-out 2-8
dynamic, framing (ppp and slip) 2-10
dynamic, ip packet routing 2-10
dynamic, ipx packet routing 2-11
dynamic, overview 2-7
dynamic, setup 2-8
dynamic, synchronous setup 2-11
IPX 15-5
LAN types 2-1
LAN, AppleTalk packet routing 2-4
LAN, IP packet routing 2-3
LAN, IPX packet routing 2-3
load balanced 6-4
multiline 6-4
PPP 5-1, 15-10
remote 6-11
serial line dedicated, setup 2-4
serial line, dedicated
serial line, dedicated 2-4
single-line dynamic IP 6-1
synchronous 5-1
watchdog 2-6
internal network number, IPX 15-4
IP address 4-1
IP address, peer 15-9
ip filter 9-1
IP global address 4-2
IP packet filtering 9-1
IP RIP 4-3
IP routing table 4-3
ipdial 5-3, 6-6
IPX
address 15-1
configuration 15-1
framing 15-6
interface 15-5
internal network number 15-4
network number 15-3
node number 15-4
packet frame 15-6
port number 15-4
RIP 15-8
route 15-12
SAP 15-6
socket number 15-4
IPX.COM 15-20, A-2
IPX.LDR A-2
IPXPPP.LAN 15-17, A-2
ISDN terminal adapter 1-2

K

keepalive, IPX 15-16

L

LAN interfaces, types 2-1
learning routes
IP 4-2
leased line router 1-2
line assignments B-1
line characteristics 10-2, 10-5
line reset command 13-2
link-layer frame type, IPX 15-6
link-raw TCP, setup 13-1

load balanced (see interfaces, load balanced)
local user record 11-2
login prompt 3-7, 3-8
LOGIN.EXE 15-17
logout 3-10
LOGOUT.EXE 15-17

M

MacTerminal 3.0 3-2, 3-6, 16-1
management, network (see also network management) 14-1
MAP.EXE 15-17
MIB
  enterprise 14-8, 14-9
  NetBlazer 14-8
  Telebit enterprise A-20
MIB.CMU A-3
MIB.TXT A-3
modem preconfiguration 10-4
modem server 1-6, 10-1
MODEMCAP.TXT A-8
MS-DOS
  using to backup system diskette 3-4
  using to preconfigure STARTUP.CNF 3-4
msglog 14-7
multiline (see interfaces, multiline)
multiport ARA server 1-7

N

NetBlazer
  command prompt 3-8
  host name, assigning 3-9
  login prompt 3-7, 3-8
  saving system configuration 3-11
  system diskette, back up 3-4
NetBlazer Configuration Utility 3-2
network management 14-1
network number, IPX 15-3
NETX.COM 15-20
node number, IPX 15-4

O

octal table, AppleTalk C-style C-1
output filtering 9-1

P

PacerTerm 3-2, 3-6, 16-1
packet filtering 9-1
packet frame, IPX 15-6
PASSWD A-4
password 6-5, 6-9, 11-3, 14-4, 14-5, A-4
password records, from a domain name server 14-5
peer IP address 15-9
permit filter 9-1
ping, IPX 15-15
port number, IPX 15-4
PPP 1-5
ppp dedicated interface backup 2-6
ppp shell, see remote shell
PPPCFG.EXE 15-19, A-2
PPPCFG.HLP 15-17, A-2
PPPCFG.MDM A-2
pppdial 5-3, 15-11
privileges 11-3
proxy ARP 8-1

R

raw characteristic group 13-1
raw connection, line configuration 13-1
raw server, starting and stopping 13-2
raw TCP link, setup 13-1
remote configuration
  files 14-4
remote destination 10-1
remote interface 6-11
remote IPX configuration 15-15
remote password file 11-1
remote shell 15-17
restricting line use 10-6
RIP (see also IPX RIP)
  IP 4-3
root password, setting 3-10
root, user id 3-10
route 1-2
  auto-route 6-3
  dynamic 1-2
  IPX 15-12
  leased line 1-2
  static 6-3
  static IP 4-2, 4-4
routing table
  IP 4-3
RTMP 16-3

S

SAP 15-6
SAP table 15-16
save local 14-4
save remote 14-4
saving system configuration 3-11
saving the IPX configuration 15-15
serial character mode 10-1
serial line dedicated, setup 2-4
server, BOOTP 14-3
server-raw, starting and stopping 13-2
service advertising protocol, see SAP
SLIP 1-5
slipdial command 2-9
SNMP
  community names 14-9
  configuration 14-8
  configuration procedure 14-10
  default settings 14-8
  sysContact 14-10
  sysLocation 14-11
  sysName 14-11
SNMP.LDR A-2
socket number, IPX 15-4
STARTUP.CNF 3-1, 14-4, A-3
  saving 3-11
STARTUP.CNF, manually editing 3-1
STARTUP.CNF, off-line editing 3-2
static IP route 4-2, 4-4
subnet bit mask 4-3, 6-10
Switch 56 CSU/DSU 1-2
switched digital network 1-2
synchronous dynamic interface, setup 2-11
synchronous interface (see interfaces, synchronous) 5-1
synchronous lines B-1
synchronous links
  AppleTalk 16-8
  dedicated, AppleTalk 16-8
  dynamic 16-9
  dynamic backup of 16-8
SYNxxx dual-port synchronous boards B-1
SYSCON.EXE 15-17
sysContact 14-10
sysLocation 14-11
syslog
  messages 14-6
  messages, sending 14-6
  messages, to remote host 14-7
  monitoring activity 14-6
syslog host command 14-6
syslogd daemon, UNIX 14-6
sysName 14-11
system diskette, backup 3-4

T

TCL.LDR A-2
Telebit enterprise MIB A-20
terminal server 1-5
testing IP configuration 4-6
TFTP 14-1, 14-3
timeout, IPX keep-alive 15-16
Token Ring 1-2
traps
  authentication 14-8
  modem 14-8

U

unreachable ICMP destination 9-1
user 14-6
  ID 6-8, 14-4
  records 14-4
user command 11-8
user destination group
user ID 11-1
user list 3-10
user privileges 11-3
user record 1-5, 11-1
user remote command 14-5
userdomain command 14-6
USERLIST.EXE 15-17

V

V.25bis dialing protocol 1-2

W

watchdog 2-6
WATCHPPP.EXE 15-21, A-2
WHOAMI.EXE 15-17

Z

zone names 16-2

Options

Supplements

90283-01

Table of Contents

Technical Support Procedures

Return for Repair Procedure Support-1
90-Day Limited Warranty Support-2

Synchronous Modem Brief

Joining the Global IP Internet

Overview Internet-1
Basic Walkthrough Internet-1
1. Obtaining an IP Network Number Internet-1
2. Registering a Domain Internet-2
3. Physical Interconnection Issues Internet-2
4. Network Service Providers Internet-2
5. Tying It All Together Internet-3
Network Service Providers Internet-3
Networking Reference Information Internet-5
Other Service Providers Internet-6

Application Notes

Obtaining Application Notes from the Technical Support File Server Notes-1

Connecting NCD X-Terminals

Connecting NCD X-Terminals Through the NetBlazer Notes-3
Required Hardware Notes-3
Required Software Notes-3
Installation Notes-3
Connecting NCD X-Terminals Directly to a Netblazer Notes-4
Flow Control Issues Notes-4
User Issues Notes-4
Initiating the X Session Notes-4

Setting Up Dedicated SLIP or PPP Asynchronous Lines

The Process Notes-7
Setting Up a SLIP Link Notes-7
Setting Up a PPP Link Notes-8

Chat Script for Annex Computers

Chat Script for Cisco Terminal Server SLIP Connection

Theory of Operation Notes-12

Telebit NetBlazer: Setting Up the MacSLIP LAP

Where to Get MacSLIP Notes-14
Installing and Configuring the MacSLIP LAP Notes-14
Wiring Diagrams Notes-14

Modifying the DTR Handshaking Cable to Facilitate RTS/CTS Handshaking Notes-15
Modifying the DTR Handshaking Cable Notes-15
Building the Necessary Adapters (adapts DTR Cable to RTS/CTS Cable) Notes-16
Building the Necessary Adapters (adapts DTR Cable to RTS/CTS Cable) Notes-16
Buying a Cable Built For RTS/CTS Handshaking Notes-17
Creating the Dynamic Interface on the NetBlazer Notes-17
Configuring the MacSLIP CDEV and the Modem for Dial-In Use Notes-18
Configuring the MacSLIP CDEV and the Modem for Dial-In Use Notes-18
Configuring the Modem Notes-19
Creating the Log-In Script Notes-20
Creating the Log-In Script for Macs Connected Directly to the NetBlazer Notes-20
Creating the Log-In Script for Dial-In Use Notes-21
Log-In Script (continued) Notes-22
Creating the Log-In Script for (Packet Mode) Callback Use Notes-23

NetBlazer – Morning Star PPP with Asynchronous Dynamic PPP Interfaces

Configuring the Sun SPARCstation IPC, T3000 or WorldBlazer, and MST PPP Notes-26
Configuring the NetBlazer Notes-31

Wollongong's Pathway to NetBlazer Dial-Up SLIP

Pathway Software Setup Notes-33
Making the Connection Notes-33
Telebit NetBlazer Setup Notes-35
Testing and Use of the Connection Notes-36
Bringing up the SLIP interface Notes-36

Setting Telebit Modems for Leased-Line Operation

Establishing the Carrier Notes-40
4-Wire or 2-Wire Interface? Notes-40
NetBlazer Note Notes-40

Telebit NetBlazer:
Using the Load Balance Command

Instructions for Setting Up Multiple Lines with Load Balancing Notes-41
Instructions for Setting Up Multiple Lines with Load Balancing Notes-41
Instructions for Disabling Load Balancing Notes-42
What You Should See When the Route Is Balanced Notes-42
Performance Notes-43
Test Data Notes-43
User Data Transfer Rate Notes-44
Alternate Procedure Note Notes-45

Technical Support Procedures

Telebit Corporation has made every effort to ensure that the product you have purchased is of excellent quality in all respects. Telebit products are rigorously tested and subjected to strict quality control procedures. However, if you experience difficulty in the use of this product, or it does not appear to operate correctly, we suggest doing the following:

- Read this documentation set. It has been provided to help you configure and use your system.
- Contact your dealer. Telebit authorized dealers are familiar with Telebit's products and should be able to help you resolve any problems that you may encounter while setting up and using the system.
- Finally, call Telebit's Technical Support at (408) 734-5200 or 1-800-TELEBIT. Before calling, please have all the following information about your unit available:
  - Product Name and Model Number
  - Serial Number
  - Date of Purchase
  - Place of Purchase

If your product should require service, we will repair or replace it under the terms of our 90-Day Limited Warranty. Please read the warranty statement included in this chapter, and return the Warranty Registration Card provided with this product.

When the 90-Day Limited Warranty period expires, Telebit will continue to service your product for the current applicable service fee.

Contact Telebit for information on our full range of support services, including support contracts and expedited repairs.

Return for Repair Procedure

The following procedure describes how to return the unit to Telebit for repair. This procedure is applicable to both in or out of warranty repairs.

1. Call Telebit's Technical Support Department at (408) 734-5200 or 1-800-TELEBIT and describe the problem. Tell the technical support representative if your unit is or is not covered by warranty. They will issue you a RMA number.

If the unit is covered by a warranty but not registered, you must submit proof of purchase. If you do not have proof of purchase or your unit is not covered by the warranty, you must send the current repair fee with your unit. The technical support representative will provide you with that information and any further instructions if necessary.

2. Pack the unit in its original container or in a sturdy corrugated box using nonstatic material such as newspaper as a cushion. Do not use highly static prone material such plastic wrap or Styrofoam packing material (beads or peanuts) as they may further damage the unit in transit.

3. Ship the unit only. Do not ship manuals, power supply or phone cord unless your technical support representative instructs you to do so.

4. Include the following information with your unit:

   Name
   Address
   City, State, Zip Code
   Telephone Number

   RMA Number
   Description of the problem
   Current Repair Fee (if applicable)

5. Ship the unit (for repair) freight prepaid to:

   Telebit Corporation
   1315 Chesapeake Terrace
   Sunnyvale, CA 94089
   Attention: Technical Support RMA #

   We recommend that you insure the unit when shipped. *Telebit will not accept units shipped* ***C.O.D.***

6. Telebit will ship the repaired or replacement product at no cost to you to any destination in the U.S.A. Telebit will choose the carrier and method of shipment. If you desire some other specific form of conveyance or you are located outside the U.S.A., you must bear the cost of return shipment and other incidental costs.

90-Day Limited Warranty

Telebit Corporation ("Telebit") warrants the hardware products and all components thereof against defects in materials and/or workmanship for 90 days from the date of your original retail purchase.

If you discover a malfunction or defect in materials or workmanship, Telebit, at its option, will repair or replace the product or component at no charge to you, provided you return it, as set forth below, during the warranty period. Telebit will furnish repair parts and replacement products on an exchange basis; all returned parts and products become Telebit's property. Repairs and replacements may be either reconditioned or new. Telebit will make the final determination as to the existence and cause of any alleged defect. If a returned product shows "no trouble found," Telebit may assess a repair charge.

Telebit does not warrant that any product will operate uninterrupted or without error. The warranty is contingent upon proper use of the product in the application for which it is intended. The warranty will be void on products which have been subjected to abuse, misuse, accident, alteration, neglect, unauthorized repair or installation; modified without Telebit's approval; subjected to unusual physical or electrical stress; or used with a power supply other than the one provided with the product. Expendable items (such as lamps and fuses) are not warranted. This limited warranty is extended only to the original purchaser and is not assignable.

THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, ORAL OR WRITTEN, EXPRESS OR IMPLIED. TELEBIT MAKES NO EXPRESS OR IMPLIED WARRANTIES INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, EXCEPT AS EXPRESSLY SET FORTH IN THIS LIMITED WARRANTY. SOFTWARE AND DOCUMENTATION IS PROVIDED ON AN 'AS IS' BASIS. IN NO EVENT SHALL TELEBIT BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, COSTS OR EXPENSES ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF ANY PRODUCT DELIVERED HEREUNDER.

Note: *Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages for consumer products, so the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may also have other rights which vary from state to state.*

Please see *Return for Repair Procedure* for specific instructions on returning products for service.

Synchronous Modem Brief

by Steven Bjork, Telebit Corporation

A brief introduction to synchronous modems and leased line usage as they apply to the NetBlazer follows. No attempt is made to describe NetBlazer operations here.

A leased line is used in a situation where a permanent link to the remote location is desired. The Internet technology is designed with the assumption that all sites are connected over leased lines, and thus have permanent, quick access to facilities attached to various places on the Internet.

A modem intended for a telephone company (telco) leased line generally is referred to as a DSU/CSU. This acronym stands for Data Service Unit/ Channel Service Unit. This type of modem allows the NetBlazer synchronous interface to connect with the telco's Digital Data Service (DDS) leased-line connection.

Many DSUs allow front-panel checks of the line continuity, usually in the form of a "remote loopback" check, where the local modem commands the remote modem to echo its input to its output. The local modem then transmits a data stream over the link and checks for any errors that may occur. Often a visible indicator allows the operator to get a quick "line ok" check this way.

A leased line usually consists of four wires. These wires must be correctly attached to the DSU before data can be carried. The DSU with a remote loopback test allows line wiring checking with no further tools. This is a valuable feature. If the modems cannot put each other into remote loopback, then the line may not be correctly wired to the DSU, or the line itself has a problem somewhere in the telco's plant. This could mean a backhoe has dug up a cable somewhere. If your previously working link fails, then the remote loopback test is a quick check of the telephone company's line.

The DSU itself often has a number of jumpers for various options. The NetBlazer can have the data connection in V.35, RS-422, or RS-232 signaling from the DSU; V.35 signaling is most common. Using RS-232 is possible with very short cables, but is often "not supported" by a particular DSU. Your first choice should be V.35, and then RS-422 or, if there is no other choice, RS-232 for your DSU/NetBlazer data link.

Another form of DSU is a fractional T1 interface. This interface splits off a portion of a high-bandwidth channel, allowing flexibility of bandwidth allocation. The NetBlazer single channel synchronous card accepts 56k baud's worth of a fractional T1 channel. The new dual channel card can connect a full T1 data rate on the first channel and up to 56k on the second channel, as well as an arbitrary fraction of a full T1 rate, for instance 512k.

The DSU jumpers should be set for a V.35 interface, 56k baud conneciton for use with the original single channel synchronous interface card.

A full T1 DSU can be used on the first channel of the new dual channel synchronous card, and up to 56k on the second channel.

Joining the Global IP Internet

by Steven Bjork, Telebit Corporation

Overview

With the availability of easily configured IP routers that can use the Public Switched Telephone System, the network of IP internets is growing phenomenally. One of the major advantages to IP networks is the global IP Internet.

This network is composed of Government networks, Research and Educational networks, and recently, commercial networks as well. All of these networks are joined by gateways, allowing the full range of IP services (such as FTP, Telnet, and applications such as X windows) to be exchanged.

The availability of sophisticated software such as compilers, X window system, and numerous other utilities makes access to the IP Internet a distinct advantage in today's internetworking environment.

This document describes the procedure for obtaining a fully supported connection to the IP Internet.

Basic Walkthrough

The elements necessary to support the internet connection are overviewed in the following items. It is assumed that you have obtained one or more of the reference materials listed at the end of this document, and understand the need for the various items as described in this note.

Additionally, you will need to consult the Network Information Center (NIC) for Network number assignment and domain registration. (The contact information for the NIC is provided in the list of Network Service Providers at the end of this document.)

1. Obtaining an IP Network Number

An officially registered network number must be obtained from the NIC. This number uniquely identifies the IP network. The NIC assigns the network number based upon the needs of your organization. The various classes of network numbers are described in the TCP/IP references listed at the end of this document.

Once the network address is obtained, individual host numbers are assigned to entities on your IP network. Each network entity must have a unique host number. Of these, one of the most important addresses that you must assign is that of your Domain Name System (DNS) server. However, you must have a network number to assign host addresses for your DNS server before you can complete the Domain Application form from the NIC (see next section).

2. Registering a Domain

A Domain Name is also registered at the NIC. The domain name uniquely identifies your organization in the Internet community. It is used in electronic mail addresses, and many other IP services. See the list of Network Reference Information at the end of this document for further information on the Domain Name System (DNS).

The NIC will not register a domain unless there are two domain servers: a primary and a secondary. Two servers are required for reliability, and it is strongly recommended that the servers be physically separated. Most often, an organization runs its own primary server, while the secondary is off-site. The off-site server can be arbitrary, and often is simply a "network neighbor." The commercial IP network providers can also act as DNS servers for smaller sites.

3. Physical Interconnection Issues

The physical connection must be supported with an IP router. The router (i.e., a Telebit *NetBlazer*) can use a telephone company (telco) leased line for high speed, or regular Public Switched Telephone System for low cost.

The router directs network traffic outside of your local organization, to and from the Internet. The flexibility of the IP protocols is especially apparent here, with numerous options available for transport and interconnection of various IP network segments. Options include optical fiber, satellite relay, microwave transmission, or common telco lines.

4. Network Service Providers

There are several organizations that can provide interconnection to the Internet. Military users generally are attached to the Defense Data Network (DDN). Research and Educational institutions often connect through the National Science Foundation network (NSFnet). Recently, commercial IP networks have been placed into operation. These networks generally have fewer restrictions on the traffic they carry as compared to Military and Research networks. A list of contacts for some of these transport agencies is provided at the end of this document.

5. Tying It All Together

Once you have obtained a network address and registered your domain, you can begin building the network connection. Coordinate with your network service provider for the appropriate access method, such as a dialup IP link using the SLIP or PPP protocols.

Your telephone company may need to install circuits if a high speed leased line is required. Once the leased line (or other access method) is in place, you can test the LAN access. Consult your router vendor's documentation (i.e., the *NetBlazer Reference Manual*) for the appropriate configuration commands.

Once your IP routers are configured for your network topology, the packets should flow.

Congratulations, you're now a member of the IP Internet community.

Network Service Providers

This section lists providers of IP network backbone transport facilities. Agents for Military, Government, Research and Education, and Commercial users are listed. The Network Information Center (NIC) is listed as well.

Government Systems, Inc.
Attn: Network Information Center
14200 Meadow Park Drive Suite 200
Chantilly, VA 22021

+1-703-802-4535
(800) 365-3642

The Network Information Center provides assignment of IP network addresses, registers domains, and operates the root name server for the Domain Name System (DNS).

Defense Information Systems Agency (DISA) Headquarters
8th and South Courthouse Road
Washington, DC 20390

Military and Government communications services are provided by DISA, formerly known as Defense Communications Agency (DCA).

National Science Foundation Network
1800 G Street, NW
Washington, DC 20550

+1-202-357-9717

The NSFnet backbone provides supercomputer access for research and educational facilities across the planet. In addition, NSFnet provides network access for government agencies.

UUNET Communications Services
3110 Farview Park Drive, Suite 570
Falls Church, VA 22042

+1-703-876-5050

UUNET offers many services, including Domain MX records and commercial Internet access.

California Education and Research Foundation (CERFnet)
10100 John Jay Hopkins Drive
La Jolla, CA 92093

+1-619-534-5056

CERFnet provides commercial IP network access.

Performance Systems International (PSInet)
P.O. Box 3850
Reston, VA 22091

+1-703-620-6651

PSInet provides commercial IP network access.

Advanced Network & Services, Inc. (ANS)
100 Clearbrook Road
Elmsford, NY 10523

Phone: 1-914-789-5300

ANS provides commercial IP network access.

SRI International
Network Information Systems Center
Room EJ291 333 Ravenswood Avenue
Menlo Park CA 94025

415-859-3695

SRI International provides anonymous FTP of online RFCs as well as having a complete hard copy collection of all RFCs ever published. Use `ftp.nisc.sri.com` for access to the RFC collection.

The following list of books and other reference material provides information on networking issues, with emphasis on TCP/IP Internets.

Internetworking With TCP/IP, Second Edition
Douglas Comer
Prentice Hall

An excellent reference for most TCP/IP internet questions. Covers such issues as network classes, domains, and routing. Considered by many as the industry "bible."

The Simple Book
Marshall Rose
Prentice Hall

The Internet Standard Simple Network Management Protocol (SNMP) is given a thorough treatment by the author. Because of the nature of managing a network with SNMP, the internet protocols are given a wring out in the text.

Computer Networks, Second Edition
Andrew Tannenbaum
Prentice Hall

A comprehensive overview of various networking implementations including TCP/IP, DECnet, SNA, x.25, and various transport agents such as ethernet, token ring, packet radio, and others.

DDN Protocol Handbook
SRI International

This four volume set contains sufficient information to code a functional TCP/IP protocol implementation. A number of Requests For Comments (RFCs) are listed in the handbook.

Request For Comments
(various authors)

The Request For Comment (RFC) is the mechanism used by the Internet Community to define protocol standards. Several sites make the RFCs available for copying from the network free of charge. Hard copy service is provided by SRI International.

SRI International provides anonymous FTP of online RFC's as well as having a complete hard copy collection of all RFC's ever published. Use ftp.nisc.sri.com for access to the RFC collection.

SRI International
Network Information Systems Center
Room EJ291
333 Ravenswood Avenue
Menlo Park CA 94025

+1-415-859-3695

Application Notes

This section contains several frequently requested NetBlazer application notes. These notes provide examples of many different NetBlazer applications. Most of them apply to earlier versions of the NetBlazer product but may be wholly or partially relevant to an individual's network.

To use these application notes most effectively, look for the note that uses setups applicable to your system. To determine their usefulness, consider the hardware, software, and applications used in the examples of the application note; compare them to your requirements.

In its efforts to provide users with the latest information, Telebit develops application notes on an ongoing basis. If you cannot find an application note in this section that is applicable to your network, review the complete set of application notes, which can be found on any of the NetBlazer Technical Support File Servers (FTP ftp.telebit.com, the Anonymous FTP server attached to TBUPDATE, and other repositories). All application notes are stored as plain ASCII files.

Obtaining Application Notes from the Technical Support File Server

You can gain access to the server that contains all of these application notes in the same manner as you would get software update information. However, the application notes are on the **/pub/ap-notes** directory instead of the **/pub/netblazer** directory.

The following instructions assume that you have already loaded the ftp software on your computer system. To obtain the application notes from the server using ftp, follow these steps:

1. From the NetBlazer prompt, enter **ftp ftp.telebit.com**, or use the IP address 143.191.3.1.
2. Log in as **anonymous**. Your passweord is your e-mail name or company name.
3. Enter **cd /pub/ap-notes**.
4. Retrieve the application note index with the command **get index.an**.
5. Select the note that you want from the index listing and retrieve it in the same way that you retrieved the index.

Note: *These notes provide examples only. They may or may not be applicable to your particular setup. They have not been tested to Version 2.0 of the NetBlazer software.*

Connecting NCD X-Terminals

Connecting NCD X-Terminals Through the NetBlazer

The Network Computing Device (NCD) X-Terminal can be used with the dial-up capabilities of the NetBlazer. This application note explains how to configure the NetBlazer when it is used this way.

Required Hardware

We performed this application with the following hardware:

- A Telebit NetBlazer with a Telebit T1600 and a Telebit T3000
- An X Server, frequently either a Sun or a DEC file server
- An NCD X-Terminal with another T1600 or T3000
- The appropriate cabling, such as RS-232 (data cabling) and RJ-11 (telephone cabling)

Required Software

Our application required installation of the following software:

- The X Consortium X Window System, which can be obtained through FTP on the Internet (from export.lcs.mit.edu), or from a preferred vendor
- The NCD Xremote software for the server (Sun and DEC RISC/VAX code is available)
- The Xremote EPROMs for the X-Terminal

Installation

X Windows

To Install the X program for this application, follow the instructions provided by the agent from whom you obtained the software. (This is not a good package to start learning UNIX with). Before you install the NCD X-Terminals, make sure the X program runs properly on your server.

NCD Software

To install the NCD software, as was done in this example, load it onto your X server. Follow the directions included with the media you ordered. The Xremote EPROMs belong on the X-Terminal, as well.

NetBlazer

This application note asks you to create a user account, to allow your remote X user to access the network that is attached to the NetBlazer. No special privileges are required for this account other than the ability to telnet to the server host.

Connecting NCD X-Terminals Directly to a Netblazer

This application works best when its serial links are run as fast as possible. The Telebit T1600 modem supports 38,400 bps, the maximum rate of the NCD16 serial port. The T3000 modem supports up to 57,600 bps. The T2500 modem supports a maximum DTE speed of 19,200 bps. There is no need to run the modem with data compression enabled. The NCD software has better throughput if the modems do not attempt data compression.

Flow Control Issues

The command **at&f9s190=0** puts the T1600 into hardware flow control. A similar mode is required for other modems. Configure the NCD X-Terminal to RTS/CTS hardware flow control, using the configuration menu.

User Issues

Our application requires that the remote file server be assigned a user login for the X-Terminal user. This user login is a standard UNIX login shell. Our example also requires that the X binary directories for X Consortium and NCD be included in the user's path.

Initiating the X Session

When ready to initiate an X session, like the one described here, use **Serial Session** on the NCD X-Terminal. This causes the modem to dial the NetBlazer. To get the NetBlazer login prompt, use the standard ATDT dialing commands. If you don't see the prompt, double check your phone number and modem settings. The correct settings allow you to login to the NetBlazer, in the normal fashion.

Next, connect a binary telnet session to your server host. This starts the xinitremote program, used by the NCD software in this example, and it initiates the X program over serial lines. The binary mode is needed to provide a full, 8-bit data path. The NetBlazer command that does this is **telnet -b host,** where host is the name (or IP address) of your X server host.

Unfortunately, there are bugs in some telnet server daemons on some host software. For example, the Sun OS4.1 has a bug that may cause your system to ignore carriage returns, when you attempt to login to your server host. The line feed command is useful, if you encounter the workstation bug, described. The command **<LF>=[CTRL]-[J]** can be used to terminate your input, if you see this carriage return anomoly.

To work around this bug, once you have logged in to your server host, you may also enter **"stty sane <lf>."** This command allows partially normal operation of your login session and still permits the binary data to flow. If you are working at a more sophisticated site, you can obtain a replacement telnet daemon. Some users report that the BSD 4.4 telnet daemon fixes the binary mode bug, described above.

Our application requires that the NCD xinitremote program be started last. This brings up the X program on the serial line. Consult the NCD documentation for the best startup and configuration files to use with the NCD xinitremote program and Xremote software.

Author: NetBlazer Technical Support
Online Editor: NetBlazer Technical Support
ONLINE APPLICATION NOTE: #08
ftp.telebit.com 143.191.3.1
Login: anonymous Password: email@address

Setting Up Dedicated SLIP or PPP Asynchronous Lines

This note details the steps required to connect a device to one of the asynchronous lines using SLIP or PPP, either attached directly or with a leased line.

The Process

1. Select the asynchronous port you wish to attach the remote device to.
2. Set the desired speed on the async port.
3. Attach the remote device to the desired port, using a null modem, if needed.
4. Use the **attach** command to create an interface name.
5. Add the necessary routes, using the interface name and the **route add** command.
6. Verify that the link works.
7. Save the configuration.

Setting Up a SLIP Link

The command sequence shown below lets you attach a device to asy10 (the first port of the first 8-port expansion board) and run SLIP at 19,200 bps. This link also lets you reach Network 143.191.19 :

```
NetBlazer:Top> configure asy speed asy10 19200
NetBlazer:Top> configure interface attach asy10 slip sl0 1500
NetBlazer:Top> configure ip route add 143.191.19/24 sl0
NetBlazer:Top> session ping 143.191.19.2
PING 143.191.19.2(143.191.19.2): 64 bytes      min/avg/max/mdev
Type ^] (decimal 29) to return to NetBlazer
64 bytes from 143.191.19.2 icmp_seq=0 time=20 ms  120/120/120/0
64 bytes from 143.191.19.2 icmp_seq=1 time=10 ms  110/119/120/2
64 bytes from 143.191.19.2 icmp_seq=2 time=10 ms  110/118/120/4
----143.191.19.2 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max/mdev = 110/116/120/3
NetBlazer:Top> save
```

Setting Up a PPP Link

If you want to establish a PPP link, you need different commands to start this connection than you do to start a SLIP link. The command sequence shown below assumes that the remote end is already running PPP and is awaiting a connection (has performed a passive open). Here is the command sequence for setting up the PPP link:

```
NetBlazer:Top> configure asy speed asy10 19200
NetBlazer:Top> configure interface attach asy10 ppp pp0 1500
NetBlazer:Top> configure ip route add 143.191.19/24 pp0
NetBlazer:Top> configure ppp activeopen pp0
NetBlazer:Top> session ping 143.191.19.2
PING 143.191.19.2(143.191.19.2): 64 bytes    min/avg/max/mdev
Type ^] (decimal 29) to return to NetBlazer
64 bytes from 143.191.19.2 icmp_seq=0 time=20 ms  120/120/120/0
64 bytes from 143.191.19.2 icmp_seq=1 time=10 ms  110/119/120/2
64 bytes from 143.191.19.2 icmp_seq=2 time=10 ms  110/118/120/4
----143.191.19.2 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max/mdev = 110/116/120/3
NetBlazer:Top> save
```

Author: Telebit Systems
Online Editor: NetBlazer Technical Support
ONLINE APPLICATION NOTE #20
ftp.telebit.com 143.191.3.1
Login: anonymous Password: Guest

Chat Script for Annex Computers

Note: *Telebit Corporation only suggests the following entry. The Corporation does not support or guarantee it.*

NetBlazer customer Britt Bassett of The Root Group, Inc. (britt@csn.org) sent the following chat script to Telebit's Technical Support Group. With it, a NetBlazer user can log in to an annex and bring up slip between (link) itself and the annex. Britt actually used the link resulting from this chat script to send it to Telebit:

```
:annex
e2,15,70,4,Xylogics, Inc.
s4,5,70,6,\r
e6,10,70,8,username:
u8,5,70,10
s10,5,70,12,\r
e12,5,70,14,password:
p14,5,70,16
s16,5,70,18,\r
e18,15,70,20,annex:
o72,Incorrect
s20,5,70,22,slip\r
e22,15,100,99,192.88.205.1.

# error state 70
# timeout hit, retry
s70,5,100,71,\r\r
e71,10,100,72,login:
u72,5,100,73
s73,5,100,74,\r
e74,5,100,75,password:
p75,5,100,76
s76,5,100,77,\r
e77,15,100,78,annex:
o100,Incorrect
s78,5,100,79,slip\r
e79,15,100,99,192.88.205.1.

# return codes
# success
r99,0
# failure
r100,1
```

Author: Britt Bassett, The Root Group, Inc., 10/7/91
Online Editor: David K. Z. Harris, NetBlazer T.S.E.
ONLINE APPLICATION #41
ftp.telebit.com 143.191.3.1
Login: anonymous Password: Guest

Chat Script for Cisco Terminal Server SLIP Connection

NetBlazer uses the following chat script to open a cisco terminal server SLIP connection:

```
# Cisco terminal server slip chat sequence.

:cisco
s1,10,666,2,\r
e2,10,20,3,ame:
s20,10,666,21,\r
e21,10,22,3,ame:
s22,10,666,23,\r
e23,10,669,3,ame:
# Uh, got a Username:, send user ID.

u3,10,666,4
s4,10,666,5,\r
e5,15,669,6,sword:
# Yow, send our password.

p6,10,666,444
s444,10,666,7,\r
e7,10,669,8,>
# Ask for slip service.

s8,10,666,443,slip
s443,10,666,9,\r
e9,10,669,10,dress:
# Fortunately this is the same as our user ID.
u10,10,666,445
s445,10,666,11,\r
e11,10,666,12,sword:
# Send our password.
p12,10,666,446
s446,10,666,13,\r
# NetBlazer thinks we made it:).
r13,0

# The 666 state is a timeout on send failure.
s666,10,999,667,Failed to send string\r
r667,1
# The 669 state is timeout on receive failure.
s669,10,999,670,Failed to receive string\r
r670,1
# The 999 state means the world has ended.
r999,1
```

1. The script logs in as a regular user with a password.
2. The script issues the slip command.
3. The cisco prompts the NetBlazer for address:
4. The NetBlazer gives it the same user name (Dynamic Interface "uname").
5. The "cisco" prompts the NetBlazer for its own password.
6. The NetBlazer supplies the same password as before.

Note: *The user ID must first serve as login to the "cisco", then as the response to the cisco "address:" prompt. Also, the password must be the same for logging into the terminal server as it is for responding to the "cisco" password for SLIP service.*

The user ID and password are both taken from the Dynamic Interface (uname and password parameters). If your site is different, you may need to

- Change the chat script
- Install a new Dynamic Interface with proper name and password or
- Change the login information on the cisco

Author: Steven Bjork, NetBlazer T.S.E. 6/10/92
Online Editor: David K. Z. Harris, NetBlazer T.S.E.
ONLINE APPLICATION NOTE # 43
ftp.telebit.com 143.191.3.1
Login:anonymous Password:emailname@site.ext

Telebit NetBlazer: Setting Up the MacSLIP LAP

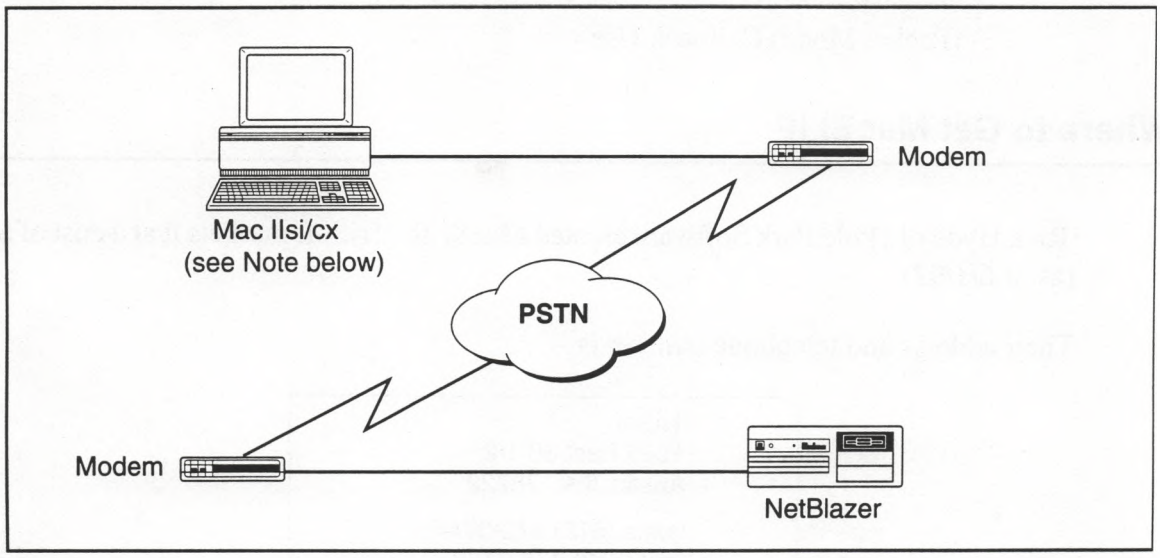


Figure 1. Setup Used In This Example

The MacSLIP LAP is an addition to the MacTCP Control Panel. It allows MacTCP to use a serial port to link a Macintosh to a NetBlazer with a SLIP link that passes IP datagrams.

The MacSLIP Control Panel configures the port speed and chooses a number of operating options.

The combination of these two programs allows your applications that use MacTCP to operate through SLIP links on remote networks.

Software requirements:

- MacTCP version 1.1 or later
- MacSLIP—The MacTCP Control Panel does not come with it.

Note: *This setup was tested with the prerelease version of MacSLIP on a Mac IIsi and a Mac IIcx running System 7 with MacTCP version 1.1, NCSA Telnet (version 2.4), and the Fetch (v2.0.6) FTP front-end from Dartmouth College. Both Macintoshes were connected by dialing into a NetBlazer using Telebit T3000 modems.*

This note is divided into six parts:

- Where to Get the MacSLIP Package
- Installing and Configuring the MacSLIP
- Wiring Diagrams (modem and direct cable connections)
- Creating the Dynamic Interface on the NetBlazer

- Configuring the MacSLIP CDEV and the Modem for Dial-in Use
- Creating the Login Script for
  - Directly Connecting to a NetBlazer
  - Dialing into a NetBlazer Using a Modem
  - (Packet Mode) Callback Use

Where to Get MacSLIP

Rick Hyde of Hyde Park Software created MacSLIP. TriSoft markets it at a cost of $49.95 (as of 6/1/92).

Their address and telephone number is

TriSoft
1825 East 38 1/2
Austin, TX 78722

voice (512) 472-0744
fax (512) 473-2122

email: info@hydepark.com

Installing and Configuring the MacSLIP LAP

Installation is simple:

1. Drag the slip and MacSLIP modules into your System folder.
2. Drag the Netstat monitor and the sample script into your communications folder.

For more detailed installation instructions, see the MacSLIP User's Manual.

Wiring Diagrams

Most Macintosh modem cables are set for DTR handshaking. To ensure continuous operation of the modem, you must use a cable set for RTS/CTS handshaking. To configure a cable in this way, you have three options.

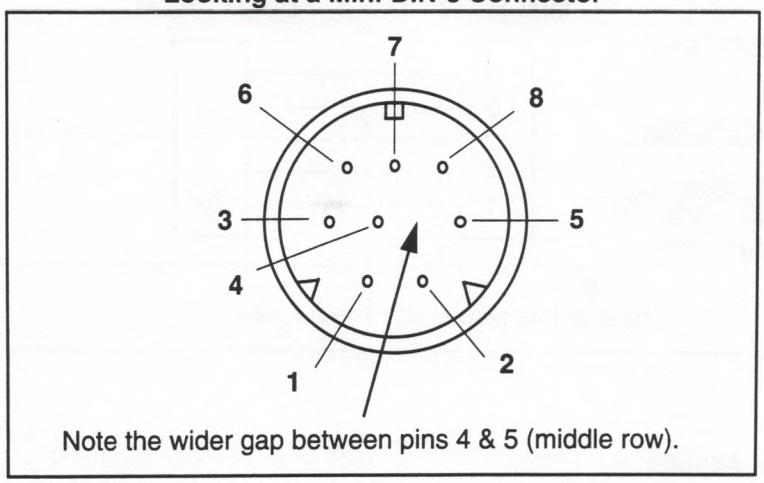
- Modify a DTR cable.
- Build the necessary adapters.
- Buy a cable already built for RTS/CTS handshaking.

Wiring diagrams for these different options appear on the following pages.

Modifying the DTR Handshaking Cable to Facilitate RTS/CTS Handshaking

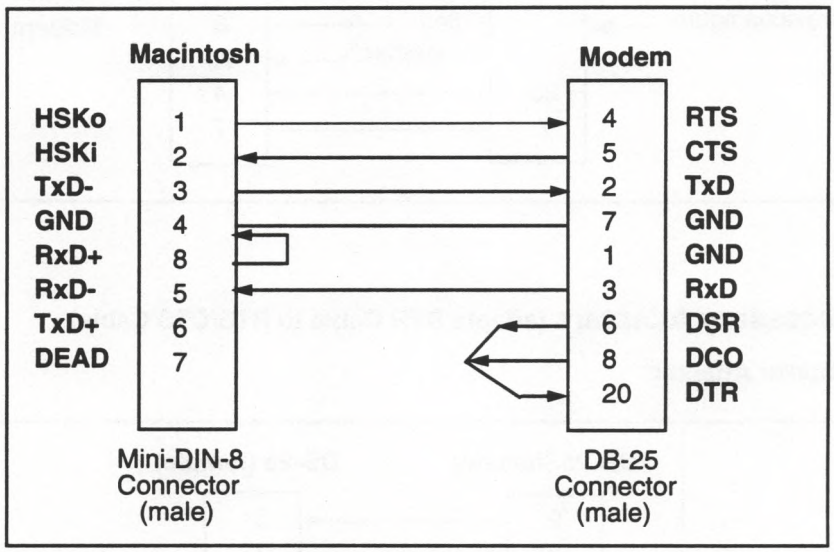
Mini-DIN-8 Pinouts

Looking at a Mini-DIN-8 Connector



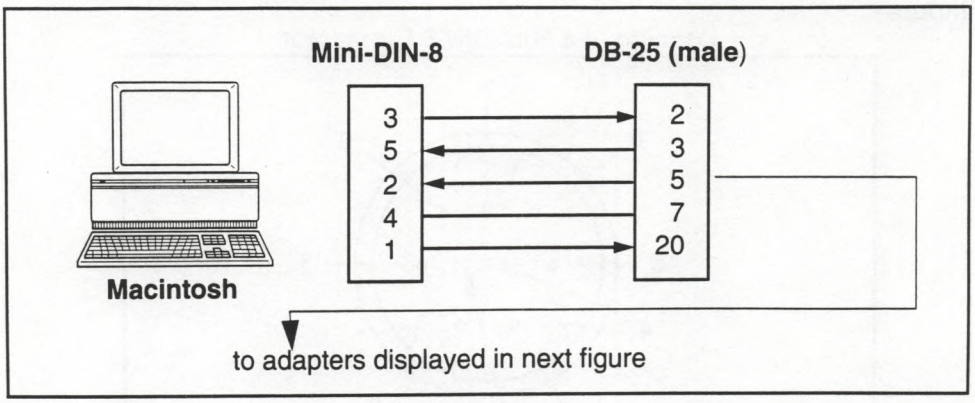
Modifying the DTR Handshaking Cable

RTS/CTS Handshaking Cable—Macintosh to Modem

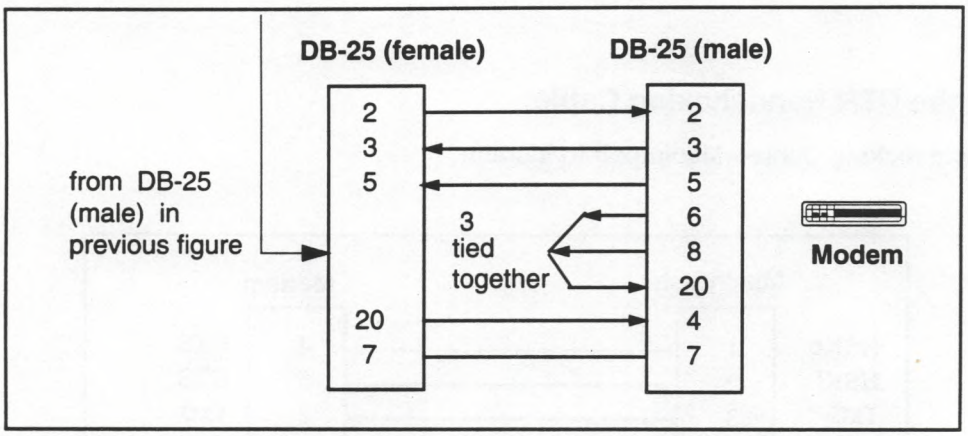


Building the Necessary Adapters (adapts DTR Cable to RTS/CTS Cable)

Typical Macintosh Serial Cable (set for DTR handshaking)

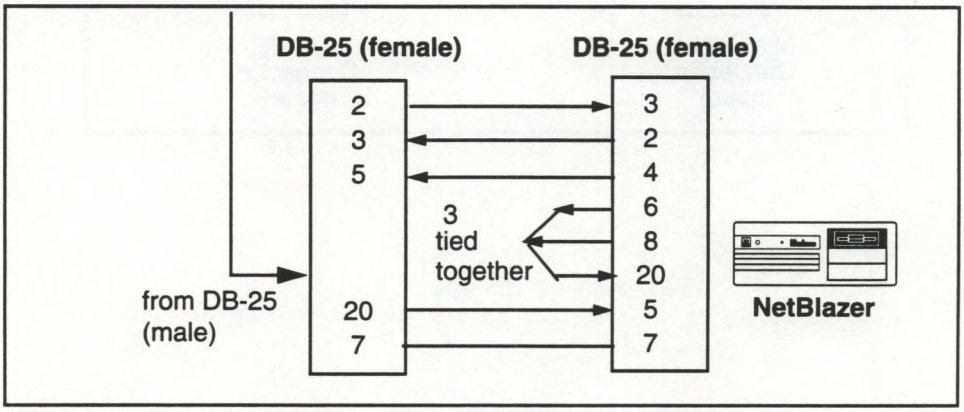


Macintosh to Modem Adapter



Building the Necessary Adapters (adapts DTR Cable to RTS/CTS Cable)

Macintosh to NetBlazer Adapter



Buying a Cable Built For RTS/CTS Handshaking

The cable that you buy should be configured according to the diagrams under the section Modifying the DTR Handshaking Cable of this application note.

Creating the Dynamic Interface on the NetBlazer

The **ipdial** command is the best way to create the dynamic interface. This command is also shown in the NetBlazer Command Reference documentation. The following is an example of the **ipdial** command:

```
wendy:Top> ipdial MacSLIP-1                          [name of dynamic interface]
Name of remote (other) system: MacSLIP-1     [the name your script sends]
Allow dial-out from this interface [y]? y    [yes, if you want callback]
Allow dial-in to this interface [y]? y       [yes lets the Mac call you]
Begin adding interface 'MacSLIP-1' ...
Chat script [ics]: null                      [use "null" for callback...]
SLIP or PPP (s|p) [s]: s                      [set the SLIP parameters]
Maximum lines to connect to remote system [1]: 1
What is the Maximum Receive Unit (MRU) [1006]: 1500
Add dynamic interface=MacSLIP-1, user=, chat=ics, using SLIP
   without crypto handshaking, max-lines=1, MRU=1500
Okay (yes|no|quit) [y]? y
[if you want callback, you'll enter the number to call the Mac back here]
Please add the information that the remote system 'MacSLIP-1'
 will use to contact this NetBlazer
Want to enter a password [y]? y               [yes, we'll use a password]
Enter the password (no echo):                [type in the Mac's password]
Re-enter the password:                        [type it in again...]
Issue a crypto handshake [n]? n               [no thanks!]
User: MacSLIP-1          privs:     dest-group:
Okay (yes|no|quit) [y]? y
Add routes for interface [y]? y
Begin adding route thru 'MacSLIP-1' ...       [use the Mac's address...]
Destination name or address/bits (Return to finish):143.191.201/32[RTN]
Metric [1]: 1
Private [n]: n
Add route destination=143.191.201.9, bits=32, metric=1, not private
Okay (yes|no|quit) [y]? y
Route added
Begin adding route thru 'MacSLIP-1' ...[RETURN]
Destination name or address/bits (Return to finish routes): [RETURN]
... Done adding dial IP
For proper 2-way communications, remote system should have:
1) Dynamic interface=, user=MacSLIP-1, chat=ics, using SLIP
   without crypto handshaking, max-lines=1, MTU<=1500
2) User=
3) Route destination=143.191.200.42, interface=, gateway=none, metric=1
Now, you delete the "full-time" (static) route....

wendy:Top> route delete 143.191.200.42/32 MacSLIP-1
```

Now, install an **auto-route**. This will only advertise the route for the MacSLIP-1 interface when the Mac logs in and delete the route when the Mac logs out again.

```
wendy:Top> dynamic auto-route add 143.191.200.42/32 MacSLIP-1
```

Finally, save all of the changes you have made.

```
wendy:Top> save
```

Configuring the MacSLIP CDEV and the Modem for Dial-In Use

After installing the MacSLIP LAP and CDEV in the System folder, execute the following instructions:

1. Open the Control Panel for MacSLIP
2. Set your port speed
3. Check the **DTR input flow control** and **CTS output flow control** boxes
4. Pull down the menu for Script
   a. Choose **set**
   b. Pick the script you want to use
5. Pull down the Log menu
   a. Choose **set**
   b. Pick a file name for the diagnostics trace log
6. Pull down the Port menu and choose the modem port
7. Pull down the Compression menu
   a. Choose **auto**
   b. Click in the field next to **MTU**
   c. Enter **1500**

Configuring the MacSLIP CDEV and the Modem for Dial-In Use

The MacSLIP package displays a button in the upper right corner of the panel labeled **connect**. This button tells you that MacSLIP is ready. Clicking on the button starts the script that you choose and starts the diagnostic trace running, writing out to a file called by the name you choose. However, before you click on that button, configure the modem using the instructions in the following section.

Configuring the Modem

Before you start the script and run the diagnostic trace, you must configure the modem. For this operation, the modem must be connected to the modem serial port on the Mac with a cable, or some combination of cables and adapters, set up for RTS/CTS handshaking, see "Building the Necessary Adapters (adapts DTR Cable to RTS/CTS Cable)" on page 4. You will also need some type of communications package to "talk" to the modem. When you "talk" to the modem, set it to the following parameters:

- Hardware (RTS/CTS) flow control, no XON/XOFF flow control
- Auto answer off if you don't want the NetBlazer to call you back (If you do want the NetBlazer to call you back, set the modem to answer after a certain number of rings.)

The following are the register settings for the Telebit T3000 used to test the system. (Use the **AT&V** or **ATN** commands with Telebit modems to view the current settings.)

```
T3000SA - Version LA3.00 - Active Configuration
B1  E1  L1  M1  Q0  T   V1  X1  Y0
&C1 &D2 &G0 &J0 &L0 &Q0 &R3 &S0 &T4 &X0
S000=0   S001=0   S002=43  S003=13  S004=10  S005=8   S006=2   S007:30
S008=2   S009=6   S010=14  S011=70  S012=50  S018=0   S025=5   S026=1
S038=0   S041=0   S045=0   S046=0   S047=4   S048=0   S050=0   S051:6
S056=17  S057=19  S058:2   S059=0   S060=0   S061=1   S062=15  S063=0
S064=0   S068=255 S069=0   S090=0   S093=8   S094=1   S100=0   S102=0
S104=0   S105=1   S111=255 S112=1   S180=2   S181=1   S183=25  S190=1
S253=10  S254=255 S255=255
```

You have just configured the MacSLIP CDEV and the modem for dial in use. In the next step, you will create the log-in script.

Creating the Log-In Script for Macs Connected Directly to the NetBlazer

In the following example, no modem was involved, only a physical cable or dedicated SLIP, leased line connecting the Macintosh to the NetBlazer:

```
#
#Let the user know that the system is starting up. Setup global
#abort action.
#
beep
on abort return 1
#
#Preset Counter 0 to 0. Send a [CR] to wake up the NetBlazer
#and let it negotiate (autobaud) to our speed. If the NetBlazer does not
#respond with a login prompt in 3 tries, abort the script.
#
setcount 0 0
label NetBlazer
flush
ifcountgt 0 3 return 0
send \r
{
ifmatch ogin: break
iftime 3 goto NetBlazer
}
#
#When you get a login prompt, then try to log in as a SLIP user
#
label user
flush
send slip\r
{
ifmatch assword: break
ifmatch ogin: goto user
iftime 20 return 0
}
#
#Send your password and wait for the ">" prompt.
#
flush
send slide\r
{
ifmatch ogin: goto user
ifmatch acket break
iftime 10 return 0
}
#
#All done, return success
#
return 1
```

Creating the Log-In Script for Dial-In Use

In the following script, MacSLIP uses a T3000 modem connected to the modem port (of a Macintosh) to call into a NetBlazer. (To see the scripting language in more detail, see the MacSLIP manual.)

```
#
#Remote Mac, dialing into NetBlazer   (Guenivere -> Zaphod)
#Let the user know we're starting up. Setup global
#abort action.
#
beep
on abort return 1
#
#Preset Counter 0 to 0. Send "AT" to wake up the modem
#and let it negotiate (autobaud) to our speed. If the modem does
#not respond in 3 tries, abort the script.
#You may need to include other commands
#here to put your modem into the correct mode.
#
setcount 0 0
label modem
flush
ifcountgt 0 3 return 0
send AT\r
{
ifmatch OK break
iftime 3 goto modem
}
#
#Dial the phone and wait for the terminal server
#to send its login banner. Some areas support
#using *70 as a dialing prefix to suppress call-
#waiting tones which will probably cause your modem
#to lose the connection. Some terminal servers
#may require you to autobaud before they will respond.
#Allow enough time for the modem handshake to complete.
#

flush
send atdt1-408-745-3889\r
{
ifmatch ogin: break
iftime 1:15 return 0
}
#
#Log into the terminal server.
#
label user
flush
send MacSLIP-1\r
{
```

Log-In Script (continued)

```
 ifmatch assword break
ifmatch Username goto user
iftime 20 return 0
}
 #
 #Send your password and wait for the ">" prompt.
 #
flush
send MacSLIP-2\r
{
ifmatch ogin: goto user
     ifmatch enabled goto end
ifmatch > break
iftime 10 return 0
}
label end
beep
beep
flush
 #
 #All done, return success
 #
return 1
```

Creating the Log-In Script for (Packet Mode) Callback Use

The following script dials the callback request modem attached to a NetBlazer, asks for a callback, then starts SLIP when the callback is made from the NetBlazer to the Macintosh:

Callback Script

```
#
#Let the user know we're starting up. Setup global
#abort action. If we abort, don't start SLIP...
#
beep
beep
on abort return 0
message " We're off and running..."
#
#Preset Counter 0 to 0. Send "AT" to wake up the modem
#and let it negotiate to (autobaud) our speed. If the modem does
#not respond in 3 tries, abort the script.
#You may need to include other commands
#here to put your modem into the correct mode.
#
setcount 0 0
label modem
message "looking for the modem..."
flush
ifcountgt 0 3 return 0
send AT\r
{
ifmatch OK break
ifmatch 0 break
iftime 3 goto modem
}

#
#Dial the phone and wait for the terminal server
#to send its login banner. Some areas support
#using *70 as a dialing prefix to suppress call-
#waiting tones which will probably cause your modem
#to lose the connection. Some terminal servers
#may require you to autobaud before they will respond.
#Allow enough time for the modem handshake to complete.
#
flush
message " configuring the modem now, and dialing..."
send ate1v1x0s95=0\r
send atdt204\r
{
   ifmatch OK break
   iftime 1:45 return 0
}
# ...wait for the where: prompt...
```

Callback Script (continued)

```
 #
{
   ifmatch CONNECT break
   iftime 1:45 return 0
}
message "Connected...waiting to request a callback..."
label where
setcount 0 0
flush
ifcountgt 0 3 return 0
send \r
{
ifmatch here: break
iftime 1:30 return 0
}
 #Log into the terminal server.
 #
message " requesting callback..."
label user
flush
send MacSLIP-1\r
message "callback has been requested, waiting for callback...
 # Wait for the callback
 #    (If you time out, start dialing again)
 #
{
   ifmatch RING break
   iftime 1:1200 goto modem
}
message " answering the phone..."
{
   ifmatch CONNECT break
   iftime 1:45 return 0
}
message " it's a modem!  *** SLIP is starting! :-)"
beep
flush
 #
 #All done, return success
return 1
```

Author: Technical Support Engineering 7/24/92
ONLINE APPLICATION NOTE # 46
ftp.telebit.com 143.191.3.1
Login:anonymous Password:emailname@site.ext
revised: 7/24/92

NetBlazer – Morning Star PPP with Asynchronous Dynamic PPP Interfaces

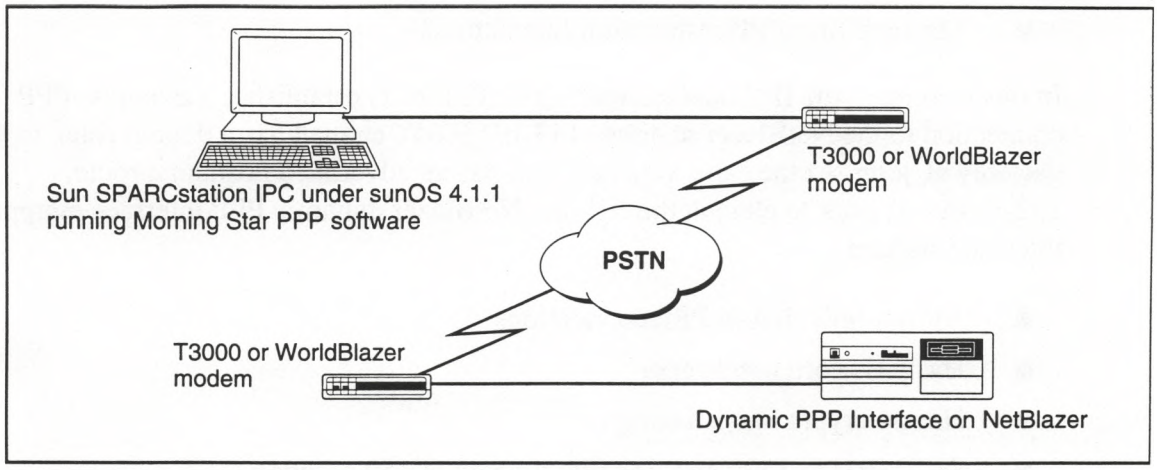


Figure 1. Setup Used In This Example

This application note is an example of how to configure a Sun IPC running Morning Star PPP software through a T3000 or WorldBlazer modem for demand dial PPP through another T3000 or WorldBlazer modem to a dynamic PPP Interface on the NetBlazer.

This note assumes that you have installed the Morning Star PPP software properly on the Sun IPC and plan to make an inbound asynchronous PPP connection to the NetBlazer.

Note: *This application note applies only to this setup. If you are trying to connect any system other than a Sun SPARCstation to the NetBlazer, refer to another application note. If you are using modems other than the T3000 or WorldBlazer, the modem settings may be different.*

Hardware and software used in this application note:

- Telebit NetBlazer (N10-1E), Software Version 1.5
- Telebit T3000 Modems, LA3.00 or later
- Telebit WorldBlazer Modems, LA5.00W or later
- Sun SPARCstation IPC, sunOS 4.1.1
- Morning Star Technologies, Inc. (MST) PPP Software, Version 1.3

The documents used to write this application note, which may be useful to you as you set up your system, are listed below:

- NetBlazer 1.5 Reference Manual and Release Notes
- Morning Star PPP User Guide, Revision 1.106
- Morning Star PPP Installation Instructions

In this example, the IPC host **chagall** (192.124.94.1) establishes a dynamic PPP connection to the NetBlazer **st_john** (143.191.9.64). **chagall** has a default route to the gateway **st_john**. At the same time, **st_john** has an advertised hostname route, 192.124.94.1, back to **chagall** through the NetBlazer dynamic PPP interface **mstppp**. The interface **mstppp**

- Allows only dial-in PPP connections
- Has password **gatekeeper**
- Has no crypto handshaking
- Sets MRU to 1500 and link idle timeout to 180 seconds

The **chagall** T3000/WorldBlazer is on device **cua**; the **st_john** T3000/WorldBlazer is on Line 11. This PPP link

- Starts only when traffic is present
- Sets the debug facility to link status messages (default)
- Sets the link idle shut down time to 180 seconds

Once started, **chagall**

- Dials the NetBlazer **st_john**
- Connects **chagall** to **st_john**
- Sends the username **mstppp** in response to the **st_john** login prompt
- Sends the user password **gatekeeper** in response to the **st_john** password prompt

Once verified, **st_john** sends back the message **Packet mode enabled**. This message signals **chagall** that the LCP negotiation has started. After the IPCP negotiation is successfully completed, the dynamic PPP connection is opened.

Configuring the Sun SPARCstation IPC, T3000 or WorldBlazer, and MST PPP

Note: *If you already have the MST PPP configuration files set up for* **Devices, Dialers, Filter, Systems, Startup, rc.local**, *do not copy .ex files (for example,* **Foo.ex** *to* **Foo**). *That action overwrites any configurations already set up (in* **Foo**, *for example). In addition, the shell* **Quick-Install.sparc** *takes care of all of these MST PPP configuration files, which is helpful to SPARCstation users.*

1. After you install MST PPP, edit the **/etc/remote** file for device **cua** as follows:

```
cua:dv=/dev/cua:br#38400:
```

2. **tip** to the T3000 or WorldBlazer, then set the modem settings as below:

For T3000 modem:

```
chagall# tip cua
connected
at&f9s0=1s7=120s48=1s51=6s58=2s59=15s61=0s63=1tq2x12&c1&d3&s1&w
OK
at&v
T3000SA - Version LA3.00 - Active Configuration
B1  E1  L2  M1  Q2  T   V1  X12  Y0
&C1 &D3 &G0 &J0 &L0 &Q0 &R3 &S1 &T4 &X0
S000:1  S001=0   S002=43  S003=13  S004=10  S005=8   S006=2   S007:120
S008=2  S009=6   S010=14  S011=70  S012=50  S018=0   S025=5   S026=1
S038=0  S041=0   S045=0   S046=0   S047=4   S048:1   S050=0   S051:6
S056=17 S057=19  S058:2   S059:15  S060=0   S061:0   S062=15  S063:1
S064=0  S068=255 S069=0   S090=0   S093=8   S094=1   S100=0   S102=0
S104=0  S105=1   S111=255 S112=1   S180=2   S181=1   S183=25  S190=1
S253=10 S254=255 S255=255
OK
```

For WorldBlazer modem:

```
chagall# tip cua
connected
at&f9s0=1s7=120s48=1s51=6s58=2s59=15s61=0s63=1s92=1tq2x12&c1&d3&s1&w
OK
at&v
WorldBlazer - SA - Version LA5.00W- Active Configuration
B1  E1  L2  M1  Q2  T   V1  X12  Y0
&C1 &D3 &G0 &J0 &L0 &Q0 &R3 &S1 &T4 &X0
S000:1  S001=0   S002=43  S003=13  S004=10  S005=8   S006=2   S007:120
S008=2  S009=6   S010=14  S011=70  S012=50  S018=0   S025=5   S026=1
S038=0  S041=0   S045=0   S046=0   S047=4   S048:1   S050=0   S051:6
S056=17 S057=19  S058:2   S059:15  S060=0   S061:0   S062=15  S063:1
S064=0  S068=255 S069=0   S090=0   S092:1   S093=8   S094=1   S100=0
S104=0  S105=1   S111=255 S112=1   S151=4   S155=0   S180=2   S181=1
S183=25 S190=1   S191=7   S253=10  S254=255 S255=255
OK
```

3. Be sure the status for T3000 or WorldBlazer in **/etc/ttytab** is set to "on:"

For T3000 modem:

```
console   "/usr/etc/getty std.9600"      sun      on local secure
ttya      "/usr/etc/getty std.38400"    dialup    on    # T3000
```

For WorldBlazer modem:

```
console   "/usr/etc/getty std.9600"      sun      on local secure
ttya      "/usr/etc/getty std.38400"     dialup   on    # WBLAZER
```

4. Copy **/etc/ppp/Devices.ex** to **/etc/ppp/Devices** and edit the file you have just created.

   For T3000 modems, add

   a. **T3000** under **Dialer**
   b. **cua** under **device**
   c. **38400** under **speed**
   d. **crtscts** under **Optional parameters**

```
#
# Dialer          device  speed          Optional parameters
#
 T3000           cua     38400          crtscts
```

   For WorldBlazer modems, add

   a. **WORLDBLAZER** under **Dialer**
   b. **cua** under **device**
   c. **38400** under **speed**
   d. **crtscts** under **Optional parameters**

```
#
# Dialer          device  speed          Optional parameters
#
 WORLDBLAZER     cua     38400          crtscts
```

   This file associates dialer types with physical devices and speeds, including EIA RS-232D hardware (RTS/CTS) flow control.

5. Copy **/etc/ppp/Dialers.ex** to **/etc/ppp/Dialers**. You do not need to edit the Dialers file. This file describes how to dial each type of modem attached to the UNIX system that is to be made available for outbound PPP calls.

   You do not need to edit or invoke the Filter file. This file describes how on-demand PPP links are to be managed, binding packet types to actions.The default settings allow any packet type to bring up or traverse the link. They also allow any packet sufficient to reset the idle timer to bring up and traverse the link, as the expiration of the idle timer could cause the link to shut down and drop the connection.

Note: *Start with a simple filter specification and add each special case only as the need arises, usually as the result of watching packet logs. Be careful with header logging and even more careful with full packet content tracing. Make the selection criteria very narrow, or the logfile will grow extremely large in a short period of time.*

6. Copy **/etc/ppp/Systems.ex** to **/etc/ppp/Systems** and edit the file you have just created by adding the following:

   a. Under **name**, enter **Internet address** or **hostname** if name can be resolved in the IPC's local **/etc/hosts** or **YP/NIS** or **DNS** cache

   b. Under **when**, enter the days of the week and times of the day when the NetBlazer can be called

   c. Under **device**, enter **ACU** so any device in the Devices file with a matching speed may be used

   d. Under **speed,** enter **38400**

   e. Under **phone-number**, enter a value to replace the \T escape sequence in the dialer

   f. Under **chat-script** , enter **expect send expect send ...**

   Use the format below with your site specific information:

```
#
#
#name when device speed phone-number chat-script
```

This is an example. It was used for calling from a Sun SPARC IPC to NetBlazer **st_john**.Use this format below with your site specific information.

```
#
# This is for calling the NetBlazer st_john
#
st_john Any ACU 38400 7453719 ogin: mstppp ssword: \qgatekeeper
```

This file describes how to connect with neighboring systems through PPP.It connects to NetBlazer **st_john**, **any** time of the day, using any device with a matching speed of **38400** bps (the maximum speed for Sun serial ports). It uses the phone number **745-3719** and a chat script login name of **mstppp** that has a password **gatekeeper**. (**mstppp** is the associated dynamic PPP interface name created by **ipdial** on the NetBlazer with the password authentication **gatekeeper**.)

7. Copy **/etc/ppp/Startup.ex** to **/etc/ppp/Startup** and edit the file you have just created by adding the following lines after the phrase **echo -n "Starting PPP daemons:"**

```
echo -n "Starting PPP daemons:"                                    >/dev/console
#
# This is for calling the NetBlazer (st_john - 143.191.9.64)
#
 pppd chagall:st_john auto idle 180
                    (echo -n ' st_john')              >/dev/console
route add default st_john 1
```

This file is a shell script run from **/etc/rc.local** to load device drivers and run the ppp daemon for calling **st_john**.

8. Add the following lines to **/etc/rc.local**. You can find these lines in **/etc/ppp/rc.local.ex**.

```
#
# Startup MST PPP software V1.3 here
#
if [ -f /etc/ppp/Startup ]; then
        /etc/ppp/Startup
fi
```

This starts **pppd** when you boot up your computer.

Note: *The MST PPP installation program has probably added the lines of code in Step 8 already. This step is meant only to confirm the correct configuration.*

9. To ensure that changes take effect on the SPARCstation ICP, enter **/etc/ppp/Startup** to test your configuration. The next time you reboot your SPARCstation, your rc.local file will start pppd.

1. Create the dynamic PPP interface **mstppp** with the **ipdial** command.

```
st_john:Top> ipdial
Name of remote (other) system: mstppp
Allow dial-out from this interface [y]? n
Allow dial-in to this interface [y]? y
Begin adding interface 'mstppp' ...
Chat script [ics]: ics
SLIP or PPP (s|p) [s]: p
Maximum lines to connect to remote system [1]: 1
What is the Maximum Receive Unit (MRU) [1500]: 1500
Add dynamic interface=mstppp, user=, chat=ics, using PPP
    without crypto handshaking, max-lines=1, MRU=1500
Okay (yes|no|quit) [y]? y
Please add the information that the remote system 'mstppp'
        will use to contact this NetBlazer
Want to enter a password [y]? y
Enter the password (no echo):      ###gatekeeper### entered (no echo)
Re-enter the password:             ###gatekeeper### re-entered (no echo)
Issue a crypto handshake [n]? n
User: mstppp            privs:     dest-group:
Okay (yes|no|quit) [y]? y
Add routes for interface [y]? y
Begin adding route thru 'mstppp' ...
Destination name or address/bits (Return to finish routes): 192.124.94.1
Metric [1]: 1
Private [n]: n
Add route destination=192.124.94.1, bits=32, metric=1, not private
Okay (yes|no|quit) [y]? y
Route added
Begin adding route thru 'mstppp' ...
Destination name or address/bits (Return to finish routes):  ###<CR>###
... Done adding dial IP
For proper communications, remote system should have:
1) Dynamic interface=st_john, user=mstppp, chat=ics, using PPP
   without crypto handshaking, max-lines=1, MTU<=1500
2) Dialout=st_john
3) Routedestination=143.191.9.64,interface=st_john,gateway=none, metric=1
```

2. Save the configuration.

```
st_john:Top> save
```

Author: Technical Support Engineering 7/6/92
ONLINE APPLICATION NOTE # 47
ftp.telebit.com 143.191.3.1
Login:anonymous Password:emailname@site.ext
revised: 01/29/93

Wollongong's Pathway to NetBlazer Dial-Up SLIP

This application note presents the suggested method for using Wollongong's Pathway Access package to dial into a SLIP connection on a NetBlazer.

Table 1. List of Names, Addresses, and Phone Numbers Used In This Example

Machine	Hostname	IP address	Phone #	Port
Pathway PC	satelite	143.191.48.2	745-3831	COM1
NetBlazer	netblazer	143.191.48.1	745-3729	Dynamic

Note: *These names, addresses, and phone numbers are fictitious. They are used in the examples of this application note to make them easier to understand.*

Software used in this example:

- NetBlazer software, Version 1.5
- Pathway Access software, Version 2.0
- ProComm Plus software, Version 2.01

Pathway Software Setup

The following setup notes assume

- You have properly installed the Pathway Access software
- You have customized the kernel

For more specific instructions, see the manual for a SLIP Client and Modem Configuration.

Making the Connection

Since the Pathway Access package does not let you log in to an intermediate device once you have made the connection, you need a terminal emulation and communications package to log in to the NetBlazer prior to the start of any TCP/IP session. ProComm Plus seems to be the best for accomplishing this task. It allows you to exit from the software without disconnecting the call in progress.

The following steps set up and run a session with a host through a NetBlazer using Pathway and Procomm Plus:

1. Load the SLIP driver.

```
C:>slip -s:7453729 -b:192 -d:1
```

This command loads the slip driver with

   a. The phone number set to **745-3729**

   b. The bps rate set to **19200**

   c. The com port set to **COM1**

2. Start the PWTCP software.

```
C:>pwtcp
```

This command starts the connection process. The modem dials the phone number entered with the slip driver. As soon as the program connects the NetBlazer, it returns a C:> prompt.

3. Start the ProComm Plus software.

```
C:>pcplus
```

When the online screen appears:

   a. Press **[RETURN]**. The screen displays a prompt from the NetBlazer.

   b. Enter your login id and your password. The system returns the message **Packet Mode Enabled**.

   c. Exit ProComm Plus using the ALT-X keystroke. If asked **Do you want to hang up?**

   d. Enter **No**. Your connection will remain intact.

You can now use any of the Pathway Access applications that you want to, *i.e.*, **TELNET, FTP, PING,** etc.

4. When you have finished and want to disconnect completely, you have two options:

   a. Let the NetBlazer timeout

   or

   b. Disconnect cleanly by going back to ProComm Plus and from the online screen enter your modem's attention string (**+++** is the default for AT command sets). Then, you can issue the hangup command, **ATH**. The NetBlazer disconnects.

The following setup starts from a factory default NetBlazer. If you already have a working NetBlazer and only want to add the dynamic interface, just follow the dialog from the **ipdial** command.

```
NetBlazer login: root

NetBlazer:Top> ip addr 143.191.48.1
NetBlazer:Top> ipdial
Name of dial IP interface to add: satelit
Allow dial-out from this interface [y]? n
Allow dial-in to this interface [y]? [RETURN]
Begin adding interface 'satelite' ...
Chat script [ics]:[RETURN]
SLIP or PPP (s|p) [s]: s
Maximum lines to connect to remote system [1]:[RETURN]
What is the Maximum Receive Unit (MRU) [1006]: 1500
Add dynamic interface=satelite, user=, chat=ics, using SLIP
   without crypto handshaking, max-lines=1, MRU=1500
Okay (yes|no|quit) [y]? y
Adding dial-in user 'satelite'
Want to enter a password [y]? y
Enter the password (no echo):<<password>>
Re-enter the password:<<password>>
Issue a crypto handshake [n]?[RETURN]
User: satelite          privs:     dest-group:
Okay (yes|no|quit) [y]?[RETURN]
Add routes for interface [y]?[RETURN]
Begin adding route thru 'satelite' ...
Destination name or address/bits (Return to finish routes): 143.191.48.2
Metric [1]:[RETURN]
Private [n]:[RETURN]
Add route destination=143.191.48.2, bits=32, metric=1, not private
Okay (yes|no|quit) [y]?[RETURN]
Route added
Begin adding route thru 'satelite' ...
Destination name or address/bits (Return to finish routes):[RETURN]
... Done adding dial IP
For proper 2-way communications, remote system should have:
1) Dynamic interface=, user=satelite, chat=ics, using SLIP
   without crypto handshaking, max-lines=1, MTU=1500
2) Dialout=
3) User=satelite
4) Route destination=143.191.48.1, interface=, gateway=none, metric=1
```

Note: *The **proper 2-way communications** message is intended for NetBlazer to NetBlazer links.*

Use the save command to save your changes.

```
NetBlazer:Top> save
```

Next, check your interfaces.

```
NetBlazer:Top> inter
NetBlazer:Top>Configure>Interface> list
Name          IP addr    MTU   type trace sent: ip  tot recv: ip  tot
satelite   143.191.48.1  1500 Dialou 0x000 Not connected
en0        143.191.48.1  1514  Ether 0x000      0    0        0    0
loopback   127.0.0.1     65535       0x000      0    0        0    0
```

Add a static route to your network, and save your changes.

```
NetBlazer:Top>Configure>Interface> route
NetBlazer:Top>Configure>IP>Route> add 143.191.48/24 en0
NetBlazer:Top>Configure>IP>Route> list
Dest            Len Interface    Gateway        Metric  P Timer  Use
143.191.48.0    24  en0                          1         0      0
143.191.48.2    32  satelite                     1         0      0
NetBlazer:Top>Configure>IP>Route> save
```

The host(s) on your network must now be taught to reach the Pathway machine (satelite) through the NetBlazer. If your host does not know how to interface with a router (through a "route add gateway" or "route add net" command), you need to add a proxy arp for the 143.191.48.2 (satelite) address in the NetBlazer. To do this, see the "ARP Commands" section in your Command Reference documentation.

Testing and Use of the Connection

Bringing up the SLIP interface

1. Connecting the Modems

   slip.exe, pwtcp.exe, pcplus.exe, and one of the applications contained in the Wollongong package connect the modems. This sequence brings up the physical layer.

```
C>slip -s:7453737 -b:192 -d:1

C>pwtcp
calling 7453737...
CONNECT 9600

C>pcplus

NetBlazer login: satelite
Password: <<password>>

Packet mode enabled

(exit from pcplus)
```

Now you can run the different modules included with the Wollongong Pathway Access package. Telnet, FTP, etc., now have access to the network host you are trying to reach.

```
C>telnet 143.191.48.100
```

Author: Charlie Ford, NetBlazer T.S.E.
Online Editor: David K. Z. Harris, NetBlazer T.S.E.
ONLINE APPLICATION NOTE #48
ftp.telebit.com 143.191.3.1
Login: anonymous Password: Guest.

Setting Telebit Modems for Leased-Line Operation

Use the modem settings shown below with the NetBlazer configured for asynchronous, leased-line (dedicated) mode. (See "NetBlazer Note" on page 40.)

For two modems to operate over a leased line, one modem must be set for Originate mode, and the other modem must be set for Answer mode. Set one modem with the Originate settings appropriate for its particular model number; set the other with the Answer settings appropriate for its particular model number. For example, to set a T1600 modem in Answer mode, enter **at&f11s61=0s51=6s58=2&w0**. The settings for Telebit modems by model number are as follows:

T3000:

Mode	Command
Originate	`at&f10&s4s2=255s61=0s51=7s58=2&w0`
Answer	`at&f11s61=0s51=7s58=2&w0`

(These settings lock DTE speed to 57600 bps on the serial interface.)

T2500 in PEP mode:

Note: *Enter both lines separately! The T2500 can parse only 80 characters on a single line.*

Mode	Command
Originate	`at~&fs51=5s52=1s54=3s55=3s58=2s64=1s66=1` `ats130=5s131=1s7=255s50=255s101=2q4e0&w`
Answer	`at~&fs51=5s54=3s55=3s58=2s64=1s66=1` `ats130=5s131=1s7=255s50=255s101=1q4e0&w`

(These settings lock DTE speed to 19200 bps on the serial interface.)

T2500 in V.32 mode:

Note: *Enter both lines separately! the T2500 can parse only 80 characters on a single line.*

Mode	Command
Originate	`at~&fs50=6s51=5s54=3s55=3s58=2s64=1s66=1s94=0s95=2` `ats97=1s106=1s130=5s131=1s7=255s101=2q4e0&w`
Answer	`at~&fs50=6s51=5s54=3s55=3s58=2s64=1s66=1s94=0s95=2` `ats97=1s106=1s130=5s131=1s7=255s101=1q4e0&w`

(These settings lock DTE speed to 19200 bps on the serial interface.)

T1600:

Mode	Command
Originate	`at&f10&s4s2=255s61=0s51=6s58=2&w0`
Answer	`at&f11s61=0s51=6s58=2&w0`

(These settings lock DTE speed to 38400 bps on the serial interface.)

Establishing the Carrier

As soon as the settings are stored in the modems, turn the power off, then back on. This starts the modems negotiating a connection.

4-Wire or 2-Wire Interface?

You can get leased lines in either 2-Wire or 4-Wire circuits. Decide which modems you want, then order the right line to go with them; or you can order a line, then buy the appropriate modems.

Many telephone companies or line providers charge you a higher fee for a 2-Wire leased line. Often, these providers are just putting a hybrid in the central office to change their 4-Wire circuit to a 2-Wire circuit. It might be easier, cause you fewer problems, and be less costly in the long run to buy a 4-Wire to 2-Wire adapter. Telebit has successfully used the Data Probe model H-2/4 Adapter with Telebit modems for this purpose. The approximate cost is $110 for each adapter. (You may want one adapter on each end of the line.) If you have further questions about their product(s), contact Data Probe at (201) 569-6464.

NetBlazer Note

The modem settings on page 39 and page 39 of this note are suitable for use with a Telebit NetBlazer port configured in asynchronous, leased-line (dedicated) mode. The following NetBlazer commands set up a NetBlazer port in dedicated (direct-connect or leased-line) mode. The first NetBlazer in this example (**NB1**) has the IP address **192.9.200.1**; the second (**NB2**) has the IP address **192.9.201.1**.

```
NB1:Top> interface attach line10 slip test10 1006 192.9.200.1

NB2:Top> interface attach line10 slip test10 1006 192.9.201.1
```

These commands create SLIP interfaces between the NetBlazers with an MTU of **1006**. After you configure the NetBlazers, use the **SESSION TALK** command to program the modems with the necessary settings. (Don't forget to save your work.)

Author: Technical Support Engineering 3/20/92
ONLINE APPLICATION NOTE #50
ftp.telebit.com 143.191.3.1
Login: anonymous Password:emailname@site.ext

Telebit NetBlazer: Using the Load Balance Command

Note: *If you are familiar with the process for manually adding dialouts, interfaces, and users, see the application note that discusses an alternate way of adding the second through last interfaces.*

Instructions for Setting Up Multiple Lines with Load Balancing

1. Decide how many interfaces that you want on a path.
2. Configure them individually in IPDIAL.
   c. Specify the MTU/MRU to be 256. (If you set it any higher, performance suffer.)
   d. Specify a SLIP connection and use defaults for all other non-routing items.
   e. Specify phone and login information appropriate for your network design.
3. Do not use the default route for balanced mode operation. Set up the routes on each interface to be the same. Make sure the destination is fully qualified with the bit mask. An example is shown below.

```
NB:Top>route add 215.215.16/24 con11
```

4. Make sure that your line configurations match those of the modems or DSUs that are being used. Also, check that the modemcap entries match. These are necessary in multiline connections because any retries created by errors make the file transfer and load balancing software less efficient.

Instructions for Setting Up Multiple Lines with Load Balancing

5. Issue the route balance command. The syntax and an example are specified below.

```
NB:Top> balance
Usage: balance <dest-addr>[/<bits>] <interface> [<interface>...]
NB:Top> route balance 215.215.16/24 con11 con12 con13 con14
```

6. Check your work with the route list balance (**rou listbalance**) and route list local (**rou listlocal**) commands to make sure that you have set up the routes correctly. An example is shown below.

```
NB:Top> rou listbalance
Dest              Len Interface    Gateway          Metric  P Timer  Use
143.191.20.187    32  multi1                        1       P 0      127
143.191.20.187    32  multi2                        1       P 0      127
143.191.20.187    32  multi3                        1       P 0      126
143.191.20.187    32  multi4                        1       P 0      127
NB:Top> rou listlocal
Dest              Len Interface    Gateway          Metric  P Timer  Use
143.191.20.187    32  multi1                        1       P 0      127
143.191.20.187    32  multi2                        1       P 0      127
143.191.20.187    32  multi3                        1       P 0      126
143.191.20.187    32  multi4                        1       P 0      127
143.191.22.0      24  en0                           1       P 0      6468
```

7. Repeat Steps 1 through 6 when setting up the remote end except substitute the remote site equivalents for your local site specification. Repeat these steps to completion. Disable **dialin** or **dialout**, if desired, on the correct NetBlazer.

Instructions for Disabling Load Balancing

1. Issue route delete commands (**route delete con**) for each route that has been balanced.

```
NB:Top> route delete con11
NB:Top> route delete con12
NB:Top> route delete con13
NB:Top> route delete con14
```

2. Check to see that all of the appropriate routes have been deleted. You can check this with the route list balance command (**rou listbalance**).

What You Should See When the Route Is Balanced

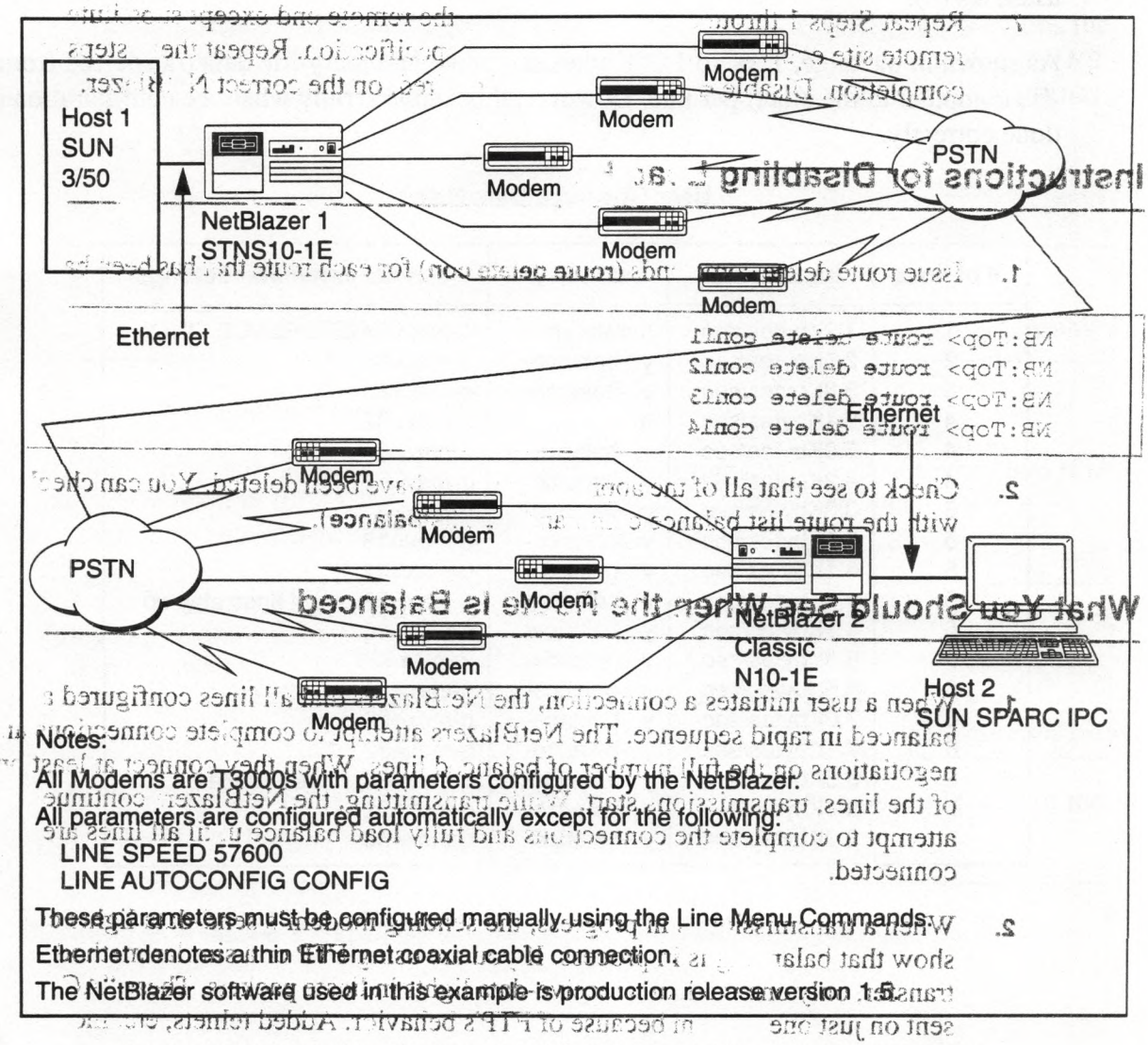
1. When a user initiates a connection, the NetBlazers dial all lines configured as balanced in rapid sequence. The NetBlazers attempt to complete connections and negotiations on the full number of balanced lines. When they connect at least one of the lines, transmissions start. While transmitting, the NetBlazers continue their attempt to complete the connections and fully load balance until all lines are connected.

2. When a transmission is in progress, the sending modem's send-data lights clearly show that balancing is in process. If you are using FTP or a similar method of file transfer, only one modem's receive-data lights indicate packets. These "ACKs" are sent on just one modem because of FTP's behavior. Added telnets, etc. modify this appearance.

The performance data listed in this section was observed in testing. Telebit does not claim that these identical results will occur with other setups. The performance indicated by this data does not represent the full or maximum performance possible in these links. FTP is a limiting factor in this observed performance. You can carry multiple simultaneous sessions across this multiline connection.

Test Data

This test runs with an FTP file transfer crossing from as few as two and as many as seven lines simultaneously. The test was successful in each of the cases. The file transfer used a 6-Megabyte file in binary format, with very little added asynchronous traffic on the data link, between two Sun workstations. Figure 1 shows the hardware setup tested.



Notes:

All Modems are T3000s with parameters configured by the NetBlazer.

All parameters are configured automatically except for the following:

LINE SPEED 57600
LINE AUTOCONFIG CONFIG

These parameters must be configured manually using the Line Menu Commands.

Ethernet denotes a thin Ethernet coaxial cable connection.

The NetBlazer software used in this example is production release version 1.5.

Figure 1. Hardware Test Setup: Data Link Between Two Sun Workstations

User Data Transfer Rate

The following table, titled User Observed Data Rate, shows the user-observed file transfer rate given by the FTP application as kilobytes transferred/duration of transfer (Kbytes/sec). However, the actual quantity of data transmitted is much greater. Just look at the ASY LIST character counts for bytes transmitted and received, both before and after the transfer—including framing info and retried bytes as well as the transferred file data. The FTP protocol is a limiting factor in this performance.

Note: *Most protocols are designed for use on fast, local connections. Many of these suffer some performance problems when used on DIALUP. They read at relatively low speed in comparison to Ethernet lines. The NetBlazer cannot make the protocols as effective as possible on your host systems for use on DIALUP lines; it can merely provide the data path.*

The parameters necessary to ensure the best transfer rates of actual user file data are shown in the table below. The best parameter cases experienced in this test are designated by asterisks (*).

As shown in the table, 1.2K to 1.25Kbytes/sec of actual binary file data transferred from one computer to the other, per line. However, this happens only when the configuration is done correctly.

User Observed Data Rate

# of lines	transfer rate	balance y/n	special parameter settings
1	1.2Kbytes/sec	n reference	q-max=8 REFERENCE ONLY
2	2.5Kbytes/sec	y -balance-	q-max=8 *
3	3.8Kbytes/sec	y -balance-	q-max=8 *
4	2.1Kbytes/sec	n	q-max=32
4	5.0Kbytes/sec	y -balance-	q-max=8 *
4	4.2Kbytes/sec	y -balance-	q-max=32
5	3.3Kbytes/sec	y -balance-	q-max=8
5	6.0Kbytes/sec	y -balance-	q-max=16
5	6.1Kbytes/sec	y -balance-	q-max=24 *
5	3.4Kbytes/sec	y -balance-	q-max=32 only 4 lines stay up
6	4.7Kbytes/sec	y -balance-	q-max=16
6	6.3Kbytes/sec	y -balance-	q-max=20
6	6.5Kbytes/sec	y -balance-	q-max=24
6	7.0Kbytes/sec	y -balance-	q-max=28
6	7.1Kbytes/sec	y -balance-	q-max=32 *
6	5.5Kbytes/sec	y -balance-	q-max=32, mru&mtu=512
7	8.4Kbytes/sec	y -balance-	q-max=32
7	8.0Kbytes/sec	y -balance-	q-max=36

In addition to these, several cases provided other data. The data that follows illustrates the performance drop off when less than the configured number of lines set up in the ROUTE BALANCE command (**balance**) are brought up properly.

# of lines	transfer rate	balance y/n	special parameter settings
7	6.2Kbytes/sec	y -balance-	q-max=32, 6 lines connected
7	4.1Kbytes/sec	y -balance-	q-max=32, 5 lines connected
6	4.9Kbytes/sec	y -balance-	q-max=32, 5 lines connected
6	3.0Kbytes/sec	y -balance-	q-max=32, 4 lines connected

Note: All configurations except the test noted on one of the 6-line cases had both the **mru** and **mtu** set to **256**.

Alternate Procedure Note

Instead of adding each interface with the **IPDIAL** command, you can use the **IPDIAL** command to create the first interface, **SAVE** it, then make the other interfaces by editing the **STARTUP.CNF** file. The following example shows the procedure on a NetBlazer named **NB**, and creates the interfaces **multi1** through **multi4**. (However, before you do this, use **IPDIAL** to create an interface called **multi**.)

1. Obtain the syntax using the **grep** command.

```
NB:Top> grep multi startup.cnf
configure dialout add multi 3888 dialout 60 0 0
configure interface dynamic add multi "alpha" #0 #0 "ics" slip 1 1006
```

2. Replace **multi1** with **multi2**, etc.

Note: *The line that begins with the words* **configure interface dynamic** *has been broken into two lines at the point in the code where you see the ... symbols. When you enter your configuration data, type all the information as one long line.*

```
NB:Top> grep multi passwd
multi:abu0FQlZ2zHUM:2:::::
NB:Top> configure dialout add multi1 3888 dialout 60 0 0
NB:Top> configure interface dynamic add multi1 "multi1" #0 #0 "ics"...
            ... slip 1 1006
```

3. Add the new users and give them a password. Use the same password for all of the multiline users.

```
NB:Top> user add multi1
NB:Top> passwd multi1
Changing password for multi1
New Password:                    [Enter the password]
Retype Password:                 [Enter the password]
NB:Top>
```

Author: Technical Support Engineering 6/16/92
ONLINE APPLICATION NOTE # 51
ftp.telebit.com 143.191.3.1
Login:anonymous Password:emailname@site.ext

TELEBIT®

First In Dial-Up Networking